REDCENTRIC MANAGED AZURE PORTFOLIO SERVICE DEFINITION

Version 1.1
01 February 2024

redcentric

AGILE • AVAILABLE • ASSURED

Contents

1. Service Overview

In today's business landscape, it's essential to have a strong cloud infrastructure to stay competitive. However, adopting cloud infrastructure and modernising it can be a daunting task, that requires technical expertise and a significant investment of time and resources. Many businesses are looking for a way to leverage the power of public cloud without incurring these challenges and expenses. This is where Redcentric empowers customers to mitigate these challenges and accelerate adoption. By partnering with Redcentric, businesses can focus on their core business objectives while not having to focus on the technical aspects of cloud management. This is especially important for businesses that require a flexible, evolving set of services to manage their transition to the cloud. Which is why at Redcentric, we believe in forming true partnerships with our customers; establishing long term relationships which allow us to deliver maximum value through a deep understanding of our customers' businesses to achieve maximum success.

We're a global technology company focused on consulting, implementation, and managed services and we specialise on accelerating time to value throughout every phase of your cloud journey — getting you to the cloud fast, allowing you to see results quickly. We aim to gain a deep understanding of your challenges so that we can fully apply our expertise in processes, applications, data, security, multi-cloud, and hybrid cloud to help meet your business goals.

An Extension of Your Team

Redcentric's Adaptive Cloud Engineering (ACE) team develop and deliver modern cloud solutions that provide a wide range of support and management options which are designed to allow your engineers to be focused on your core business objectives, thereby maximising your agility and efficiencies, while keeping costs to a minimum.

Redcentric ACE provides access to cloud expertise through a process of agile based, ongoing sprints to continually remediate, modernise, evolve, and improve your environment.

A True Partnership

Our flexible, collaborative approach to professional services allows you to dynamically change scope and priorities based on business needs while collaborating side-by-side with our highly skilled Redcentric ACE cloud experts to build, migrate, optimize, and transform your environments.

Leveraging the world's leading public cloud services, we can simplify migrations, safeguard security, ensure quality of delivery, and guarantee the requisite degree of responsive support and focused advice.

Redcentric wide portfolio of Hybrid Cloud Services provides solutions across multiple public cloud vendors, our own shared cloud, private cloud, managed network, and other technology focused services which ensures we deliver value to you, for all your technology-based requirements and help drive better outcomes for your business.

Microsoft Services

Our Microsoft Services help address the challenges that businesses face when running Microsoft-based technology workloads within any environment; our cloud-specific services provide support for the implementation and operation of Azure and Modern Work (Microsoft 365) environments. Each Azure service can be consumed independently to ensure we can support your business through any changes and align to your business needs and budget appropriately, with all services shown here:

Redcentric Microsoft Services

ACE SERVICES

Advisory	Modern Workplace 365	Managed Azure	Professional
Cloud Readiness	Foundations	Foundations	Migrate & Optimise
Governance	Enable	Enable	Re-Platform
Well-Architected	Operate	Govern	Transform
	Modernise	Operate	
		Modernise	

Plan	Manage	Secure	Optimise	Automate
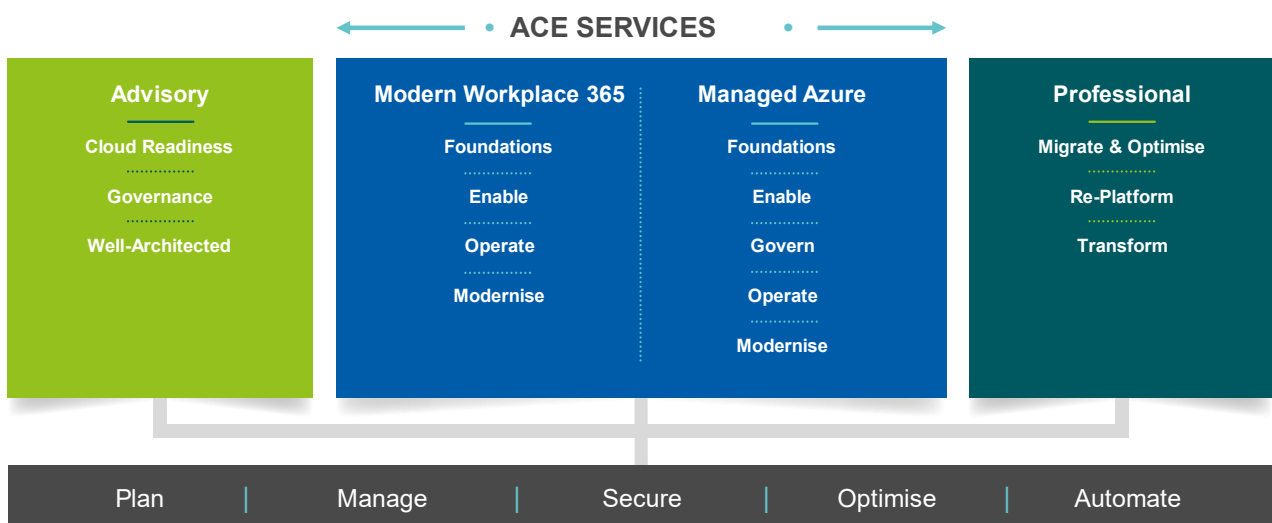
2. Our Approach

Redcentric have been working with Azure since its release in 2010, over which time we have gained extensive experience and knowledge which we utilise, along with the Microsoft Well Architected and Cloud Adoption Frameworks, to ensure every Azure environment we design, and build is aligned to best practice. Onboarding of existing Azure environments require a discovery be performed to assess how they align to our standards, any deviations found are outlined for remediation work to be carried out.

Landing Zone Considerations

- ✓ Operating Model Alignment
- ✓ Baseline Reference Architecture
- ✓ Hub & Spoke or Mesh
- ✓ Naming Conventions
- ✓ Compliance Requirements
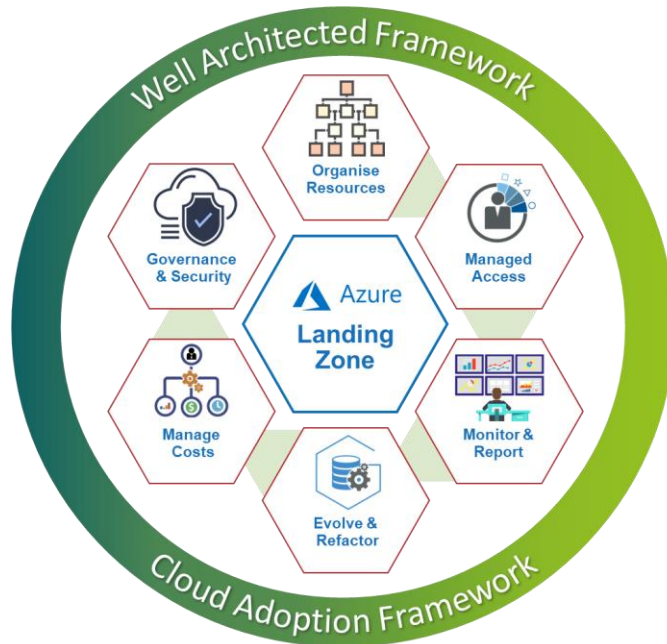- ✓ Security Requirements
- ✓ Monitoring Requirements
- ✓ Retention Policies
- ✓ DR, HA & Risk Mitigation
- ✓ RACI Matrix
- ✓ Deployment Timeline
- ✓ Long Term Objectives

Managed, Co-Managed or Unmanaged
*Foundations is considered Unmanaged

In situations where the customer chooses to co-manage resources, any resources not created or altered by Redcentric will need to be onboarded before Redcentric considers them managed.

2.1. Public Cloud is a Journey, Not A Destination

As organizations increasingly use the cloud to store and manage their data, it's important for decision makers to remember one key point: The cloud isn't a destination. It's a journey, and it's one that plays an essential role in enabling digital transformation for any organization.

For Redcentric, the cloud isn't simply where your organization goes with its data and applications; it's the experience required to optimize the use of your apps and data, no matter where they reside. Increasingly, that means embarking on a journey to a hybrid cloud, a mixture of public cloud, private cloud and on-premises infrastructure that best serves your organization's IT needs by extending the cloud experience across the enterprise, which is where a partnership with Redcentric shines the most with our approach illustrated below:

A Cloud Journey with Redcentric
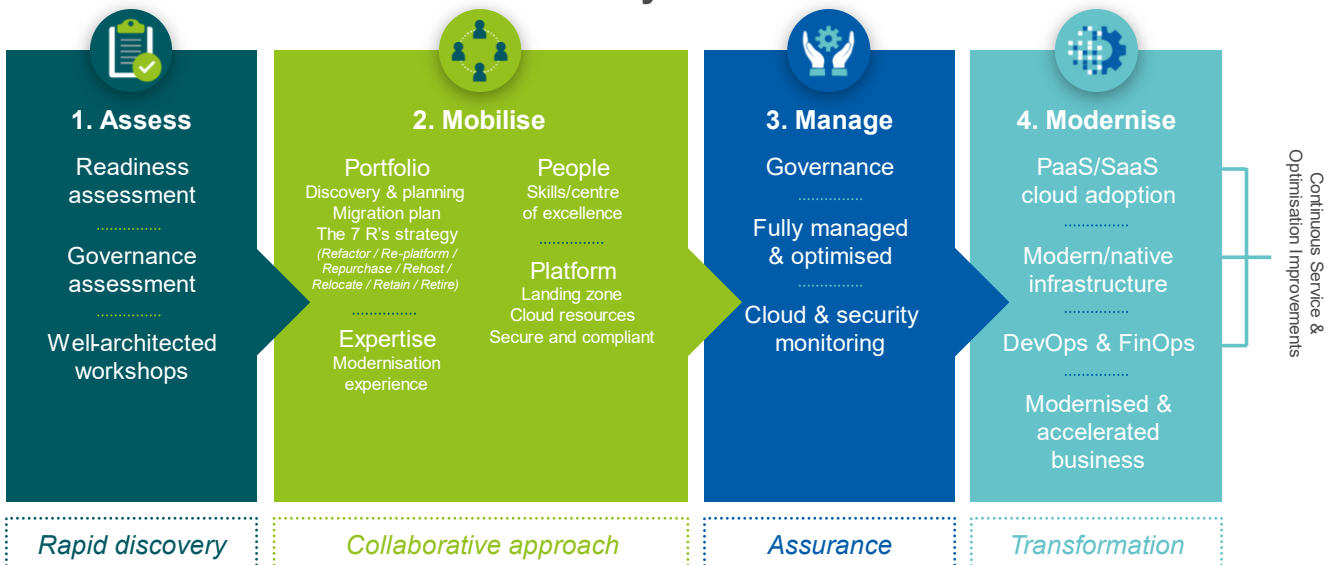
3. The Redcentric ACE Team

Redcentric ACE Support for Microsoft Azure functions as extension or in place of the customer's internal team, providing specialized resources to deliver ongoing service and support for a customer's business. Redcentric provides customers with Azure-certified solutions architects and engineers who are ready to deliver always-on support and expertise to our customers, 24x7x365.
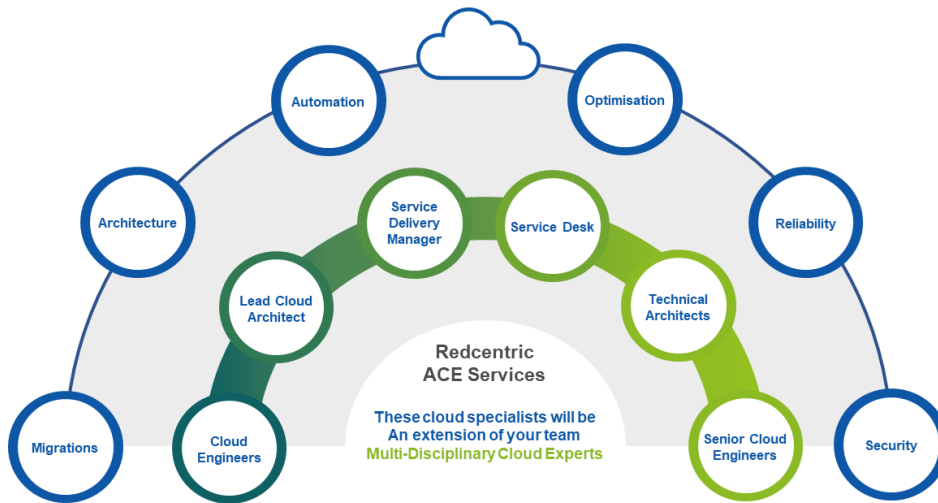
Azure-certified Service Desk

Redcentric's Service Desk are a group of cloud-specific and certified hands-on engineers that support many different cloud infrastructures, providing wide-ranging troubleshooting and support to help ensure the customer cloud environments have maximum uptime, then escalating within Redcentric's ACE teams or Microsoft in the unlikely even we are unable to resolve the issue.

Azure-certified Engineers and Architects

The Service Desk team is backed by a team of Azure-certified ACE engineers and architects, responsible for monitoring and operational support for Azure subscriptions covered by the Managed Services offering.

Account Manager

Customers will be assigned an Account Manager to help guide them through the Redcentric support process and oversee the day-to-day management of accounts, including service, change and incident management.

Service Delivery Manager

Service Delivery Managers handle the Service Reviews, which are included automatically depending Azure environment size. This provides customers an opportunity for regular governance sessions of your environment's performance, and to review operational information such as the status of backups, patching and antivirus.

The review may include items such as:

- Support tickets.
- Monitoring alerts.
- Upcoming change or maintenance events.
- Product roadmap updates.

Onboarding Manager

When purchasing a Redcentric ACE Managed Service, the onboarding manager is the personal contact for assistance with the Redcentric onboarding process. As a dedicated guide, an onboarding manager will work with key stakeholders to coordinate the resources and project management associated with the deployment of a customer's Azure environment.

4. Azure Managed Service

4.1. Overview

Whether you're looking to spur innovation and agility with Azure cloud, lower costs or build operational efficiencies, the Redcentric offerings below delivered by our ACE teams can help guarantee success Azure or across multiple platforms if you use Multi or Hybrid-Cloud.

Our ACE Microsoft Azure certified cloud experts put cutting-edge capabilities to work for your business. We apply deep expertise in cloud strategy, cloud-native development, containers, application modernization, and workload management to help you accelerate innovation with Microsoft Azure.

As you pursue this evolution, you need more than just support. You need help understanding how to scale your IT organization in an agile world, how to transform your environment and how to streamline your operating models. This is why many organizations need more than the traditional managed services models, which is constrained to fit the boundaries of the past.

This is why we've packaged the complexities of the cloud journey into 5 independent managed offerings to support a customer at every stage of their journey, while achieving the best of both worlds with a cost-efficient standardised approach and the flexibility needed in the cloud, as depicted here:

Foundations	Enable	Govern	Operate	Modernise
✓ CSP benefits ✓ Redcentric Service Desk ✓ Self-Service Portal ✓ ACE Escalations	✓ Managed Platform ✓ Managed Network, Firewalls & Edge Services ✓ Managed Storage ✓ Tagging, Monitoring & Reports ✓ Platform Monitoring ✓ PaaS Configuration & Management ✓ Platform Optimisations	✓ Cost Monitoring & Optimisations ✓ Compliance Assistance ✓ Resource Consistency ✓ Assisted regulatory compliance ✓ Security governance ✓ Azure discounts ✓ Reporting	✓ Deployment & Scaling configuration ✓ Managed OS ✓ Managed VM's ✓ Patching Schedules ✓ Disaster Recovery Configuration ✓ OS Monitoring	✓ Automation ✓ Containerization ✓ Modernisation ✓ OS-Upgrades ✓ Bespoke Dashboards ✓ Application Support & Integration ✓ Training ✓ Third Party Management
Free for CSP Customers	*Percentage Based + Minimum Fees*	*Fixed Fees*	*Per-VM/OS Fees*	*Per-Block-of-Hours Fees*

4.2. Service Geographic Availability

At this time, Redcentric customers can deploy resources to all Microsoft Azure regions existing along with Redcentric Managed Services as of the publication date of this document. Foundations is only available for sale in the United Kingdom and Europe where the primary tenant must reside, though customers can still deploy resources to all other Microsoft Azure regions. This excludes some of the Microsoft Azure Sovereign Regions (e.g., Azure Gov and Azure China). Some Azure regions are available only to customers with specific billing addresses in that region. Contact a Redcentric if you have questions about a specific region.

4.3. Redcentric CSP benefits

Azure Cloud Solution Providers (CSPs) like Redcentric offer several benefits that make them the ideal partner for businesses looking to leverage cloud infrastructure. Unlike purchasing directly from Azure, CSPs provide a more personalized and tailored service that is based on the specific needs of individual customers. This includes customized pricing and support plans that are designed to meet the unique demands of each business.

Moreover, CSPs offer a single point of contact for all Azure services, which makes it easier for customers to manage their cloud services. CSPs also provide additional services and support beyond what is available through Azure, such as migration assistance, security assessments, governance services, and ongoing monitoring and management. These services can help businesses optimize their cloud infrastructure and ensure that they are getting the most out of their investment in Azure.

Additionally, partnering with a CSP provides a more flexible billing model that allows customers to pay monthly for only the services they use, rather than committing to an annual contract. This can help businesses manage their costs more effectively and avoid unexpected expenses.

Overall, working with a CSP like Redcentric can provide businesses with a more streamlined and efficient experience when adopting cloud infrastructure. Through personalized support, a single point of contact, additional services, and flexible billing options, CSPs can help businesses optimize their cloud infrastructure and achieve their business goals. Thus starting with our free Foundations offering paves the way to accelerated success.

4.4. Service Offerings & Benefits

Azure – Foundations

A customer's cloud modernisation journey typically starts here, with Redcentric's Public Cloud (Azure) Foundations. Foundations is suitable for all Microsoft CSP subscription types, can be unmanaged, co-managed, or fully managed, and gives customers prioritised access to Redcentric's project-based Adaptive Cloud Engineering teams, as well as the CSP benefits:

- ✓ Provisioning Advice
- ✓ 24/7 Service Desk
- ✓ Self-Service Portals
- ✓ Escalated Microsoft Support

Azure – Enable

Enable empowers customers to focus on their business objectives instead of the day-to-day. It comes in two tiers, Enable provides baseline tooling, monitoring, and access to ACE certified cloud specialists for day-to-day operational support and management. Enable takes the everyday platform complexities from an IT team, to deliver standardised operations and incident response to ensure that the customer's Azure environment is:

- ✓ Getting Operation Excellence
- ✓ Securely Connected
- ✓ Monitored Platform

Azure – Enable+

Enable+ builds on Enable, adding optimisation capabilities to improve performance, automation, efficiency, and reliability with industry-leading tooling. Enable+ is best paired with the Govern service to ensure customers achieve the highest level of success with their investment to ensure that the customer's Azure environment is:

- ✓ Well-Architected
- ✓ Optimised & Efficient
- ✓ Resilient
- ✓ Organised & Standardised

Azure – Govern

Govern is a consultancy-led offering with fixed fees to support the planning, compliance, budgeting, deployment, operation, and success of an Azure environment. We provide an integrated audit and consulting approach for reviewing and advising organisations on their usage of the Azure platform to ensure that the customer's Azure environment has:

- ✓ Budget Controls & is Cost Optimised
- ✓ Policy Management
- ✓ Compliance Remediation Assistance
- ✓ Compliant Infrastructure

Azure – Operate

Operate will protect customer's VM's & OS's to make the most critical and time-consuming server tasks easy to complete. Designed to be multi-cloud, Operate provides patch management for Customer's VM workloads to ensure that the customer's Azure environment is:

- ✓ Robust & Up to Date
- ✓ Monitored OS's
- ✓ AV Management

Azure – Modernise

Modernise is not a whole service offering but an addon of customisable deliverables in the form of pre-purchased hours. This is the best way to accelerate your business's cloud journey to deliver complex cloud operations via Redcentric ACE experts. Whether you desire a deeper technical relationship to drive outcomes or need assistance handling your architecture's complexity, the ACE team can assist an organisation in finding the right solution to ensure an Azure environment is:

- ✓ Automated & Modernised
- ✓ Achieving the Lowest TCO
- ✓ Integrated with Customised Monitoring
- ✓ Supported for DevOps

4.5. Azure Advisory Services

For many businesses, the move to public or private cloud seems out of reach as they have neither the resources nor the expertise to define a successful cloud migration strategy. At Redcentric, our Consulting and Advisory Services team brings the world's best cloud experts together to help shape your business and deliver outcomes with a cloud solution built according to best-practice architecture design and processes.

We'll start with a thorough analysis to understand your needs and identify opportunities to help you excel. From assessment to ideation and true innovation, we work alongside your team, providing the guidelines, guardrails, and expertise you need to be successful.

Each advisory offering is based on Azure industry-leading frameworks, extended with many years of Redcentric expertise to accelerate a customer's business objectives and success.

Cloud Readiness	Governance	Well-Architected
✓ Workload Ideal Placement ✓ Workload Right Sight Sizing ✓ Storage Right-sizing ✓ Platform/Workload Estimates ✓ Biggest Implication Recommendations ✓ Highlight High-level Risks	✓ Review Provisioned Resources, Monitoring, Optimisations & Tradeoffs ✓ Cost Reporting & Optimisations ✓ Compliance Assistance ✓ Resource Consistency ✓ Assisted Regulatory Compliance ✓ Security Governance ✓ Process Measurement ✓ Review Security & Compliance ✓ Review & Advise Policies ✓ Resource Consistency ✓ Deployment Acceleration Policies ✓ Azure discounts	Includes Everything In Cloud Readiness & Governance PLUS: ✓ Performance Efficiency & Reliability ✓ Monitoring, Review, Selection & Trade-offs ✓ Foundations Review, Workloads Architecture, Change Management, & Failure Management ✓ Sustainability ✓ Region Selection, Alignment-on-demand, Software Architecture, Hardware, Services Process & Culture ✓ Operation Excellence ✓ Organisation, Prepare, Operate & Modernise
2-Day Engagement with up to a month of workload scanning if needed, usually depending on workload peak/troughs.	**2-5 Day Engagement based on Cloud Adoption Framework, with a workshop at the end to go through the output and educate key stakeholders**	**Start with a free 4-hour workshop, then a 1-3 Week Engagement based on a Well-Architected Framework, with a workshop to agree objectives, then workshops to go through the output and educate key stakeholders**

Cloud Readiness Assessment

For customers moving applications into the cloud, the Cloud Readiness Assessment's in-depth discovery and design service delivers a robust target architecture and adoption plan. This service is required when the environment exceeds 10 applications, 20 source machines, or five discreet workloads in scope. Redcentric solutions architects work with customers to define the scope and agree-upon a price for the project, or alternatively, the cost of this assessment can be deducted from any work or services taken post completion.

Governance Assessment

One-off governance assessments help organisations to assess their current governance posture and identify future improvement needs to build or contribute to the governance roadmap. This service is consultancy led with a fixed price that can be offset by savings it brings. It will address security baselines, cost management, identity management, resource consistency, and deployment acceleration, in line with the MVP policies recommended in Azure's CAF.

Well-Architected Workshops

The Azure Well Architected Review by Redcentric helps take the guesswork out of making sure your existing solutions on Microsoft Azure meet industry best practices for security, availability, and operational excellence.

The Well Architected Review starts with a free 4-hour workshop, which typically expands into a 1-3-week engagement depending on what is needed, this allows Redcentric ACE experts to quickly review a customer's environment to provide immediate guidance and create a list of opportunities for improvement. The engagement aligns with the 5 pillars of the Microsoft Well-Architected Framework (Cost Optimization, Operational Excellence, Performance Efficiency, Reliability and Security).

4.6. Azure Professional Services

Adaptive Cloud Engineering (ACE) Professional Services

Eliminate technical debt, fix flawed security, or bring disparate data together with our IT security professional services. When your technology environment is working for you, your company can focus on getting ahead rather than on what holds you back. Our experts design and build cloud solutions that move your business forward.

Using cloud-native approaches based on leading DevOps practices, we help you modernize your applications and data, build in the leading security solutions and deploy everything on the right cloud infrastructure for maximum effectiveness. We've assembled a professional services team that brings you expertise for leading applications, data architectures and technologies, and security best practices – across every major cloud platform.

We make keeping up with rapidly changing cloud technologies our business, so you can get the most out of yours.

Technical additional services can be used for Transformative projects with fixed outcomes to specific T&M activities such as CI/DC Pipeline assistance which can carry additional monthly fees. In addition, set-up fees may apply.

Build & Migrate	Re-Platform	Transform
✓ Evaluate an existing asset and establish a migration plan to Rehost	✓ Evaluate an existing asset and review possible Refactor or Rebuild options	✓ Application Walkthrough: The customer to provide a guided walkthrough of their application components with the ACE teams
✓ Landingzones creation & standardization if needed	✓ Establish if a POC is needed	✓ Explore dependencies, features & options for possible Re-Architect
✓ Lift and Shift workloads or Create New	✓ Model the performance, cost, access, and operational capacity of the change	✓ Set Innovation Goals
✓ Replicate the functionality of an asset into the Landing Zone infrastructure	✓ Either POC or Deploy improved asset	✓ Provide Modernisation solutions or options
✓ Review the performance, cost, access, and operational capacity of an asset	✓ Replicate the functionality of an asset into the Landing Zone infrastructure	✓ Establish if a POC is needed
✓ Optimise asset based on review output	✓ Monitor and review the improved asset	✓ Innovation Phasing to minimise risk
✓ Ensure an asset is ready for ongoing operations	✓ Ensure an asset is ready for ongoing operations	✓ Monitor and review the improved asset
✓ Roadmap possible improvements		✓ Ensure an asset is ready for ongoing operations
✓ Highlight high-level risks		

Build & Migrate Projects

Redcentric Azure Migration Services provides a comprehensive consulting package allowing customers to leverage a team of experts across Infrastructure, Database, DevOps, Networking and Security.

Migrating workloads & production services to Azure can be challenging & costly if poorly executed. Although it's relatively easy to undertake a "lift & shift" migration to Azure this rarely delivers on transformation & ROI requirements. Ensuring a best practice deployment & appropriate governance controls is often overlooked as part of migration planning.

Our services follow the successful deployment of a Landing Zone. We assess migration workloads & move a cloud-native operating model to ensure a maximum return of a migration to Azure. Our typical approach focuses on move groups aligned to an application/service line while optimising along the way for maximum success.

Re-Platform Projects

If you're looking for quick wins with a migration solution that gets your workload onto the cloud, with minimal code changes, consider re-platforming. This involves porting your application's components to a new runtime platform where your application's features and functions stay the same, and you can take advantage of the cloud's inherent cost savings and scalability, with minimal effort. Plus, you can continue to derive value from your legacy solution.

Transformative Modernisation

Our Azure Modernisation Consulting package is for customers who wish to modernise an application using Azure native services without making a wholesale redevelopment to the application.

Migrating & modernising applications to leverage Azure native services requires a number of different skills & extensive experience. Understanding how to create best practice approaches & solutions for handling micro-services & replacing legacy components with Azure services will require the experience of a partner who has been through the process before & works closely with Microsoft to apply best practices.

5. Flexible ACE Migrations

Wherever you are in your cloud journey, whatever business outcomes you would like to solve, whichever workloads you would like to migrate, we'll meet you there and simplify and manage your path forward with our end-to-end cloud services.

Working alongside your team, we'll help you understand your options, identify, develop and deploy solutions that help you achieve smarter business outcomes, then migrate and manage your Azure cloud solutions so that you can focus on innovation and modernisation.

To launch Azure services successfully, service design, onboarding and transition will be required to prepare and test both the environment and the managed services processes. The Redcentric ACE team will undertake several workshops to discuss and confirm each element of the service, to ensure all parties are aware of roles and responsibilities in advance of service launch.

Service transition and onboarding covers areas such as ticket management setup, platform readiness with knowledge share, and finalising all ITIL practices. A test and acceptance criteria are captured and signed off, to allow for the Modern Workplace service to commence.

After service launch, Redcentric uses a formal service transition framework as the basis to carry out acceptance into service procedures, for new services landing into managed services. We typically engage at the initial stages of a project to ensure service operation adoption and readiness is planned and carried out correctly. This materializes as follows:

- To review designs, build and test artefacts to ensure supportability.
- Attend change review boards to gain early sight of changes by way of knowledge acquisition.
- To witness and validate designs and builds are delivered as proposed and intended.
- Complete operational into service documentation, training and runbook enablement, which is required as part of the service hand-over.
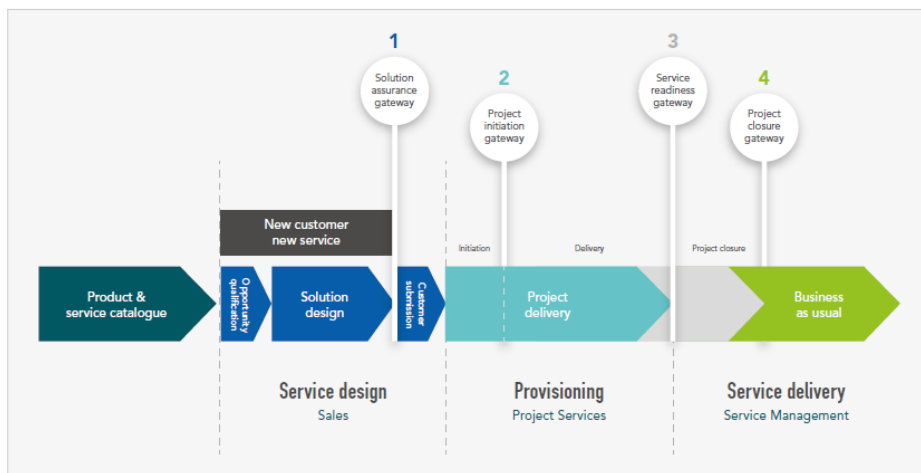
5.1. Initial Tenant Setup

If a customer is new to Azure then Redcentric can help get a customer's cloud journey started with our Azure ACE Implementation Service. To facilitate a move to Azure, we are able to offer the following services to get started.

Initial setup and configuration of essential Azure Products to best practice standards, this includes:

- Tenant Setup: creation of Azure Tenant, license provisioning, configuration of domains & setup of administrative accounts.
- Core Identity Configuration: creation of core identities to be used within Azure Cloud Environment. New identities can be created entirely in cloud, or a hybrid environment can be configured with an on premise Active Directory Domain Services using Entra ID Connect.
- Exchange: best practices configuration of mail flow rules, connection filters, anti-spam & phishing policies, auditing policies, and more.
- SharePoint & OneDrive: basic external sharing & access control configurations to ensure data is secure post migration.
- MS Teams: assistance with the deployment of MS Teams to end users and some basic tools to assist with driving adoption.
- Endpoint Manager: get devices enrolled in Intune to begin endpoint management.
- Best Practice Analysis

5.2. Migration Support

Post Migration, Redcentric are able to provide the appropriate services to get a customer's AZURE tenant to a state suitable to begin or modernise a customer's cloud journey.

The following services are available to assist post migration:

- Migration support is available for all environments*, including but not limited to:
  - Identity migrations from on-premises AD, existing Entra ID tenants or third party IAM providers
  - Data migrations from on-premises servers, existing Azure tenants, or other cloud platforms
- Modernisation, upgrades, development support, pen testing, security reviews and services or optimisations via assessments.
- Integrations with other cloud platforms to support Hybrid & Multi-Cloud designs.

*Most migrations will require admin level access to the existing environment to facilitate, with read access to existing configurations as a minimum.

5.3. Service Transition and Early Life activities

Should either Foundation, Govern, Operate, or Modernise be onboarded, there are several key differences post migration before the offerings can be considered active.

During the Design phase, Service Onboarding will cover the following activities:

- An introductory meeting, run by the Redcentric Service Delivery Manager (SDM) allocated to the customer's account.
- Engagement with the Redcentric Service Management team to run through how the customer will be onboarded, and what service management functionality and processes will be applied, and what information will be needed in order to set up the various Redcentric systems, SMAX and My Services portal correctly.
- How service engagement will work, for example, will individual sites be logging issues/requests directly with Redcentric or will there be a centralised first line triage function within the customer's organisation.
- If there is a requirement to implement a B2B link between the Redcentric and the customer's ITSM systems, and how this will be implemented.
- Provision of collateral which will enable the customer to communicate the above processes internally.

The Redcentric Transition Programme Governance process provides a series of quality gateways from the perspective of operational support and service management, to facilitate a seamless transition of services from the customer's existing provider to Redcentric. The governance framework provides three quality gateways with standardised criteria against which the project is reviewed, before being approved to proceed to the next phase.

The illustration below shows the steps and actions that are followed in the service transition.

Service Transition Model
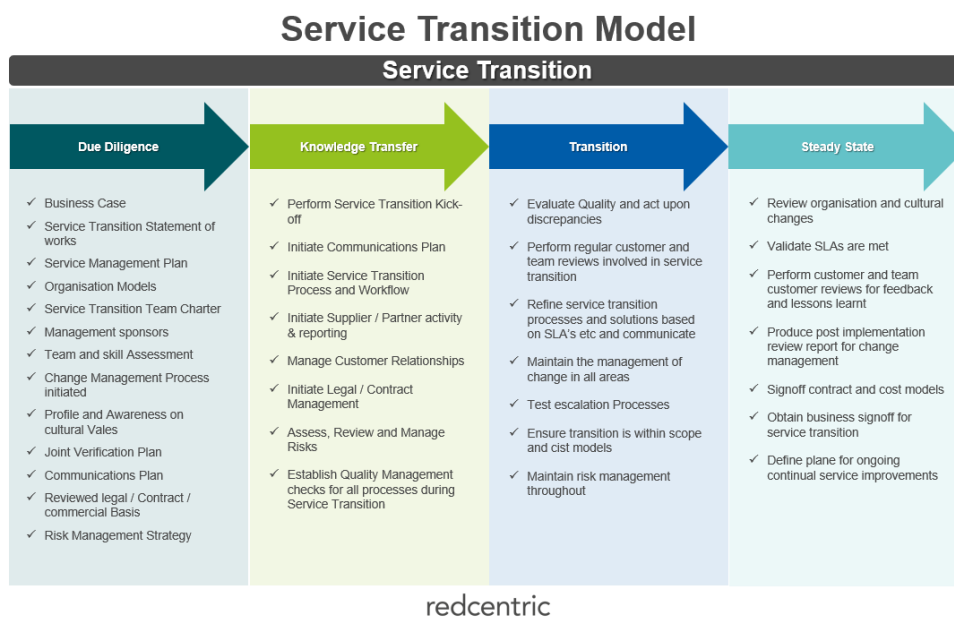
6. Scope of Managed Azure Offerings

The matrices below outline what is included along with who is considered primary for the Redcentric's Managed Azure services.

Scope Key:

✔ **Included**, as **Redcentric with primary responsibility** and customer with secondary should information or testing be needed, though if the requirement is complex, a chargeable professional project may need to be created.

✔ **Included**, except the **Customer is primarily responsible** with Redcentric providing basic support, configuration & reasonable assistance to the customer with analysis and resolution of issues, if the requirement is complex, a chargeable professional project may need to be created.

➕ **Addon**, for common activities which are typically done as a project.

Complex – Is used to describe an activity that takes multiple days to complete and requires chargeable professional services.

6.1. Service Provisioning

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Access to Microsoft Self-Service Provisioning Portal Foundation customers only.	✔					
Microsoft Escalation Support • 9x5 for Foundations • 24x7 for Enable & above Escalated support to Microsoft engineers and access to proactive cloud enablement services.	✔					
Tenant and Subscription Provisioning	✔					
Service Desk • 9x5 for Foundations • 24x7 for Enable & above Access to the Redcentric ITSM platform and L1 Service Desk Analysts for first-line fix or resolution.	✔	✔	✔		✔	✔
Telephone/Remote Support All Support/Managed Services are delivered remotely unless on-site engineering is contracted separately.	✔	✔	✔		✔	✔
Redcentric ACE Teams 9x5 Standard, 24x7 Available Access to Redcentric ACE Teams for L2-4 incidents, changes, requests, & resolutions for many of the deliverables stated in the scope.		✔	✔		✔	✔
Redcentric ACE Consultative Engagement 9x5 Only Either for proactive scheduled engagements, thought leadership or recommendation activities.				✔		
Landing Zone Deployment & Standardisation Using existing templates, policies and code to standardise and automate the deployment of new subscriptions		➕	✔			➕
Onsite support This is a bespoke, chargeable addition.						➕

6.2. Identity Management

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Entra ID Identity & Access Group Management For Admin level accounts only, for Managed user accounts, see Modern Workplace 365.		✓	✓			➕
Subscription Identity & Access Permission Management To ensure admin-level security access is consistence across subscriptions and resources		✓	✓			➕
Managed Application Registrations, Managed Identities & Apps Deployment of pre-defined templates or workshopped configurations		✓	✓			➕
Identity Risk Baseline Reviews Discover and define processes to manage exceptions to the baselines needed for Entra ID.				✓		➕
Access Review Auditing any accounts that access, service, develop or manage Azure resources.				✓		➕

6.3. Best Practices and Architecture

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Azure Architecture Design, Strategy, and Standards Design of Azure environment deployment based on analysis of each application and requirements						➕
Azure Architecture Diagrams Of existing Azure Infrastructure On-demand visual depictions of a customer's current Azure deployments						➕
Azure Architecture Reviews & Recommendations Environment review conducted by Certified solution architects focused on delivering operational stability, security and performance.						➕
Supplier Management Including Day-to-Day Problem Reporting, Liaison, and Escalation.						➕
Guidance on Upcoming Technologies Guidance on new public cloud technologies from Azure experts.						➕

6.4. Cloud Management

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Resource Naming & Tagging Using either workshopped naming conventions or those pre-defined.		✓	✓			➕

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Azure Storage Management Supports all Azure storage account types.		✅	✅			➕
Management of Azure Network and Edge Services Such as gateways, firewalls, load balancers, and WAF's etc.		✅	✅			➕
Private End-Point Management		✅	✅			➕
Automated Power-Down Scheduling Advised but not required to achieve additional cost savings.			✅			➕
Management of Key Vaults The customer always owns all Keys/Certs.		✅	✅			➕
Azure Backup Including the configurations of the backup policies dictated by the customer, along with recovery assistance within Azure.		✅	✅			➕
Compute Performance Optimisations Based on customer requests or the output from the Redcentric ACE Governance team via the Govern Service.			✅			➕
Network Optimisations Based on customer requests or the output from the Redcentric ACE Governance team via the Govern Service.			✅			➕
Workload Size Optimisations Based on customer requests or the output from the Redcentric ACE Governance team via the Govern Service.			✅			➕
Storage Optimizations Based on customer requests or the output from the Redcentric ACE Governance team via the Govern Service.			✅			➕
Ideal Workload Placement Recommendations Based on customer requests or the output from the Redcentric ACE Governance team via the Govern Service.			✅			➕
VM Scale Sets & Grouping Policies Advanced scale set and grouping configuration, monitoring and alerting.			✅			➕
App Services Configuration & Integration.						➕
Appliance Stand-Up Deployment of Pre-Defined Template		✅	✅			➕
Appliance Management Dependent on the supportability of the OS and application the appliance runs.			✅			➕
AKS Management						➕

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Our AKS management service provides: ✓ Service deployment ✓ Version upgrades ✓ CI/DC pipeline config, support and change for infrastructure only Monitoring integration						
Azure SQL as a Services Configuration & Deployment Configure + basic management of initial deployment, advanced management is an additional service as seen under optional Managed Database Service.			✅			➕
Infrastructure build-out services: Get infrastructure-as-code templates						➕

6.5. Governance & Security

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Budget Setting and Budget Alerts Agree on budget thresholds and set alerts/actions should they be breached.				✅		➕
Budget Forecasting A review of the optimisation tools and recommendations for controlling spend.				✅		➕
Cost Analysis and Recommendations Azure Advisor Review: Work through the advisories and agree actionable items.				✅		➕
Optimisation & Ideal Workload Placement Recommendations Recommend the ideal placement of workloads for cost and security.				✅		➕
Resource Utilization Reviews With the focus often on growth, auditing resource effective utilization can drive tangible savings.				✅		➕
Resource Consistency Reviews Workshopped reviews of policies, tagging, documentation and regular engagement, our ACE teams will drive consistency throughout a customer's infrastructure.				✅		➕
Data Storage Location / Retention and Process Reviews To determine if the storage is an appropriate use of block, object, database for data types, or is cost optimised across storage tiers, lifecycle and archiving methods.			✅	✅		➕
Deployment Acceleration Acceleration through centralisation, consistency and standardisation across templates (Transformation).						➕

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
IT Chargeback & Showback for Azure Consumption A standardized IT chargeback and showback enables organizations to understand and effectively allocate how various divisions, business units or cost centers are consuming IT services.				➕		➕
Cloud Application and/or End-Point Protection Standard Policy Management inside Azure Examples such as Defender for Cloud are included for assigning and managing templated policies and agents. See Core Competencies for supported security platforms.				✔		
Cloud Application and/or End-Point Protection Custom Policy Management inside Azure Examples such as Defender for Cloud are included for creating, assigning and managing custom policies and agents. See Core Competencies for supported security platforms.						➕
Cloud Application and/or End-Point Protection Outside Azure See optional services for details.						
Microsoft Sentinel Setup + Configure of the Sentinel platform, management is an additional service as seen under optional MDR / SOC services.						✔
**Application Vulnerability ==Management== **(Providing Defender for Endpoint is setup) identification and patching remediations of vulnerabilities for supported applications (Cloud Application and/or End-Point protection required)..					✔	➕
OS Vulnerability Patching Remediation of identified vulnerabilities (Cloud Application and/or End-Point protection required).					✔	➕
Blueprint & Policy Definition Creation Customising existing or creating new Azure blueprints to align with compliance requirements.				✔		➕
Blueprint & Policy Definition Assignment Assigning existing Azure blueprints to align with compliance requirements.				✔		➕
Compliance Score Remediation Assistance Getting to 100% compliance can seem an impossible task as some requirements can be unattainable, the ACE team will work closely with the customer to build a roadmap, drive remediation, identify false				✔		➕

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
positives and eliminate non-compliance.		✅	✅			➕
Compliance measurement for SLO/SLA purposes Compliance monitoring against security standards using native functionality e.g. NIST, CIS, PCI, etc.				✅		➕

6.6. Cloud Operations

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
OS Management (Windows + Red Hat) Our OS management service provides: VM & OS deployment, VM configuration, OS hardening, OS patching, network support & monitoring integration. See service requirements for supported OS's.					✅	➕
Patching Schedules, Maintenance Windows & Patch Groups Modify schedule/maintenance windows or patch groups as requested.					✅	➕
Patching Errors Troubleshoot patching errors					✅	➕
Setup Azure Update Management Setup of OS-level patching, leveraging the Azure Update Management services for Azure VMs.					✅	➕
Custom Pre- or Post-Scripts Create custom pre- or post-scripts to apply before and after patching.					✅	➕
Disaster Recovery Configuration VM & OS configuration to a pre-configured recovery vault and update monitoring integration. Initial setup and Management of Disaster Recovery is an additional service.					✅	➕
AV Agent Management Installation and configuration of agents along with ensuring policies are correctly applied.					✅	➕
Microsoft SQL Server Setup & Configuration Setup + Configure + basic management of initial installation, advanced management is an additional service as seen under optional managed database service.					✅	➕

6.7. Monitoring

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Default Monitors & Dashboards Template-driven dashboards deployed and configured.		✅	✅			➕

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Custom Monitors & Dashboards Bespoke dashboards to fit all business infrastructure needs. Multiple monitoring solution options are available.						➕
OS Monitoring Supported OS's only, see service requirements for details.					✓	➕
Application Monitoring Possible additional charges for application agents.		➕	➕		➕	➕
Agent Monitoring Configuration Configuration of Redcentric standard monitors for incident ticket creation.		✓	✓			➕
Platform Availability Monitoring Setup dashboard and alerts.		✓	✓			➕
Baseline Security Configuration Monitoring and Notification Alerts are configured for security baselines defined in workshops to notify of drift against objectives.				✓		➕
Policy Adherence/Drift Alerting & Reporting Standard Alerts are configured for policy baselines defined in workshops to notify of drift against objectives.				✓		➕
Policy Adherence/Drift Alerting & Reporting Bespoke Alerts are configured for alert/reporting baselines defined in workshops to notify of drift against objectives.				✓		➕
Updates to Cloud Monitoring On-demand changes to the configuration of Redcentric standard monitors.		➕	➕	➕	➕	➕

6.8. Reporting

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Deployment of Standard Reports Template-driven reports configured and scheduled.		✓	✓	✓	✓	➕
Customised Reports Template-driven reports are configured and scheduled.						➕
Patch Compliance Reporting On-demand report of patch compliance detail.						➕
Monthly Spend Reporting By Usage / Service Regular reports are provided based on standard templates or the custom output of the Govern service. (Scheduled)			✓	✓		➕
Policy Compliance Score Reports Regular reports are provided based on standard templates or the custom output of the Govern service. (Scheduled)			✓	✓		➕

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Run Reports on a Scheduled Basis and Provide Malware / Vulnerability Detection Reports (Based on the agreed schedule and dependent on the application and/or end-point protection software used).				✅		➕
Azure Resource Usage Regular reports are provided based on standard templates or the custom output of the Govern service. (Scheduled)			✅	✅		➕
Application Patching Tooling Asset lists, (Deployment Collections) list of all assets currently in scope as well as their current collection memberships and deployment windows. (Scheduled)						➕
Cost Reporting Against Baselines Regular reports are provided based on standard templates or the custom output of the Govern service. (Scheduled)			✅	✅		➕
Cloud Security Benchmarks and Compliance Reporting (Azure Secure Score, Defender Policies) Based on initial workshop output and benchmarked against objectives. (Scheduled)				✅		➕
Annual Assurance Assessment Based on initial workshop output and benchmarked against objectives. (Scheduled)						➕
Annual Risk Assessment Prioritized list of risk scenarios mapped to processes and technical controls. (Scheduled)						➕
Trending Analysis						➕
Infrastructure as Code Drift Reporting				✅		➕

6.9. Business Review Activities

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
Quarterly Service Reviews A customer's service delivery manager reviews reporting that summarises their account usage details. **Note** - Included at monthly Redcentric service spend above £1,500		➕	✅	✅	➕	✅
Quarterly Business Reviews A customer's account manager delivers a quarterly business review that details spending and operational actions of the prior three		➕	✅	✅	➕	✅

Scope Inclusions	Foundations	Enable	Enable+	Govern	Operate	Modernise
months and plans activities for the next quarter. **Note** - Included at monthly Redcentric service spend above £1,500						
Consultative Engagement to Engage Key Stakeholders to Drive Governance Forward				✅		
Roadmap Reviews In-depth roadmap reviews for Redcentric offers and Azure products						➕
Monthly Stakeholder Engagement				➕		➕

6.10. Combining Service Offers

Customers can take a single service for a single subscription to taking all services for all subscriptions. It is recommended to take equal services for the subscriptions that need them, though not required.

7. Associated Redcentric Services

Redcentric Managed Azure is built upon Microsoft's Azure platform, with the main goal to Modernise IT for organisations that want to focus on growth and not keeping the lights on. While not a requirement, Redcentric prides itself on being able to cover all business requirements end to end no matter the platform, thus this service compliments or can be complimented by the following:

- Business Voice & Collaboration
- Modern Workplace 365 (M365)
- Managed AWS
- Managed Windows Server
- Managed Linux Server
- Managed SQL Database
- Citrix Virtual Desktops
- M365 Virtual Desktops
- Managed Recovery Services
- Network & Connectivity
- HSCN Connectivity
- Managed Backup (Acronis / Veeam Based)
- Managed SIEM / Secure Operations Centre (SOC)

Advanced Monitoring

A number of additional advanced monitoring services are available that can improve and maintain user experience and compliance. Small examples of these services include:

- Custom tooling
- Synthetic monitoring of web application transactions & real-user monitoring
- Application performance monitoring (APM)
- Log management

Hybrid Connectivity and Integration

Redcentric provides hyperscale cloud connectivity services to facilitate hybrid and multi-cloud configurations, along with critical HCSN connectivity. Please request the Hyperscale Connect services service guide for additional information.

Managed SQL Server & Database

We will perform monitoring, support and health checks using a set of in-house developed monitoring and maintenance packs that we install on all Redcentric managed instances of Microsoft SQL and Azure SQL instances.

Modern Workplace 365

The Modern Workplace 365 Service represents the future of work, where complexity and risk are minimised, and productivity and collaboration are maximised. This service extends beyond the traditional Managed M365 offering, encompassing a comprehensive modernisation service with digital workspaces and dedicated end-user support.

Small example of these services include:

- Managed Entra ID
- M365 Backup
- Intune Management
- Device Management
- Application Support
- End User Support
- AVD Management
- IT Modernisation

The above services are only those relevant to Managed Azure and is not a complete list, for a complete list please see the Redcentric website.

8. Redcentric ACE Azure Core Competencies

The following table enumerates the core Azure competencies supported by Redcentric ACE Engineers. All Azure cloud services outside of those listed below are to be considered reasonable endeavours and may be subject to additional billable time (including training time, as applicable) in order to troubleshoot/support.

Azure Service	Service Type
Virtual Machines (VM)	Compute
VM Scale Sets (VMSS)	Compute
Batch	Compute
Reserved Instances (RI)	Compute
Azure Kubernetes Service (AKS)	Compute
App Service Environment (ASE)	Compute
SQL database	Data & storage
Azure Storage	Data & storage
Azure SQL	Data & storage
Azure SQL – Managed Instance	Data & storage
Managed Disks	Data & storage
Import/Export	Data & storage
Redis Cache	Data & storage
Cosmos DB	Data & storage
Search	Data & storage
Virtual Network	Networking
Traffic Manager	Networking
ExpressRoute	Networking
Azure DNS	Networking
Load Balancer	Networking
VPN Gateway	Networking
Application Gateway (& WAF)	Networking
Azure Sentinel	Security
CDN	Media & CDN
Azure Backup	Hybrid integration
Azure Site Recovery (ASR)	Hybrid integration
Entra ID (Formally known as Azure AD)	Identity & access management

Azure Service	Service Type
Multi-Factor Authentication (MFA)	Identity & access management
Azure Active Directory B2C	Identity & access management
Azure Active Directory Domain Services (AADDS)	Identity & access management
Scheduler	Management
Automation	Management
Log Analytics	Management
Key Vault	Management
Security Center	Management
Application Insights	Management
Blueprints	Management
Policy	Management

9. Service Requirements

This table lists items that are required to effectively deliver the services described in this document.

Required Item	Description
Hybrid Licensing	Customer is responsible if using Azure Hybrid Use Benefit
Key Stake Holder Contact Details	Periodically update the list of the customer's engineers who will use Redcentric services.
User Training	Provide training to the customer's users, clients, and suppliers to follow Redcentric procedures to report incidents or make requests.
Customer Resources	Make staff available to work with Redcentric resources during the handling of an incident or request
Existing Documentation	Provide Redcentric with all documentation, information, and knowledge that it requests in relation to the cloud environments supported.
Microsoft Support	Current in support or Extended support Windows OS assets
Patching Window	An agreed and defined re-occurring maintenance window for automated patch installation and remediation activities
Reboot Window	Reboots are permitted within the agreed maintenance windows
Internet	Outbound internet access for reporting and patching
Access Documentation	Provide Redcentric engineers with sufficient access, as defined by Redcentric to all cloud accounts supported.
Ticketing	All Priority 1 incidents are logged, and the client must follow up with a telephone call into support

9.1. Co-Management Requirements

This table lists items that are requested to effectively deliver a Co-Managed service for maximum success.

Required Item	Description
Teams Channel	Communication is the key to success for Co-Management, thus a Teams channel will be setup for smooth communication.
Service Delivery Manager	Normally only assigned based on the size of the customers environment, but becomes a requirement for Co-Managed subscriptions which could need additional charges for small environments.
Agreed RACI	Depending on the granularity required for management responsibility, an agreed RACI will be required.
Change Tracking & Logging	Change tracking and logging will be required

9.2. Subscription Management Requirements

As a part of the ACE Support for Microsoft Azure offering, Redcentric will be required to perform actions in a customer's Azure environment as a trusted partner. Redcentric cannot fulfil our role as a customer's managed service provider without the correct level of access and permissions. Redcentric takes a customer's trust and security seriously and has integrated safeguards into our management service to avoid abuse of these services, leveraging Redcentric corporate identities (along with the built-in security features like MFA credentials, password rotation, etc.). If Redcentric is unable to secure the appropriate level of access required to deliver management services, Redcentric professionals will be unable to deliver managed services in an at-scale manner using automation services and consistent tool sets for the global team of engineers.

Owner/contributor access

To deliver our Managed Services for Microsoft Azure, Redcentric requires "Owner" or "Contributor" permissions to all Azure subscriptions under our management. Several of our support offerings and/or tools require that the Owner/Contributor account be configured as an "organizational account" rather than as a "Microsoft account." If a customer is unable or unwilling to provide Redcentric with an organizational account setup for Owner/Contributor permissions, some support services may not be available or may be limited in scope.

The Owner/Contributor account credentials will be stored within a secure password repository at Redcentric and used by the Redcentric ACE teams during support, troubleshooting, deployment and other similar activities.

Azure Active Directory Service Principal Names (SPN)

Redcentric requires the configuration of SPNs to enable our management services to access resources that are secured by an Entra ID tenant . During onboarding activities, the user will be presented with an Entra ID application to consent to the required permissions for Redcentric to access resources within a tenant.

Redcentric SPNs are assigned a "least-permission levels" model, where Redcentric has defined the access policy and permissions, authentication and authorization to deliver programmatic access to resources within that subscription, enabling a host of automation services to deliver ACE Support for Microsoft Azure. SPN credentials are stored securely in an Azure Key Vault within an Azure subscription used by Redcentric for management services. The keys are encrypted at rest and in transit.

10. Customer Azure Environment Access

Azure Managed & CSP Customer Resource Access Methods

Redcentric can deploy multiple ways to access and manage a Customer's Azure Tenant, Subscriptions and Resources to best fit a customer's operational and compliance requirements. When Hybrid managed services are needed, multiple methods can be used depending on the platform being managed.

Access Method Options:

1. Traditional access via a VPN to an Azure Gateway or firewall, that can be enhanced with enforced Bastion access and is best suited for none CSP or on-site customers that need managed services.
2. Entra ID B2B guest users and native user accounts can be used, primarily when doing project work where time limited access is needed to complete work that spans both the Entra ID Tenant and specific Subscriptions.
3. Via the Cloud Service Provider partner portal after accepting Redcentric as a customer's CSP, this access method is rarely used unless agreed prior, and the customer is notified every time access is granted this way.
4. Azure Lighthouse is the most common and secure access method, allowing for continuous management of a customer's Subscriptions and Resources, while all actions are tracked via named users in the activity log.

Security Policies Enforced for Admin Access:

- Multi-Factor Authentication.
- Assigned permissions to groups, using the principle of least privilege.
- Logging enabled to track access and actions.
- No access to customers data without prior permission.
- Azure Privileged Identity Management (PIM) / "Just in Time access", is used for Azure Lighthouse access to customer Subscriptions and Resources for best practice and compliance adherence.

Optional Access Considerations:

Entra ID / Tenant access is not granted by default via Azure Lighthouse, though is often needed to carry out maintenance on monitoring tools, AKS, and Managed Identities. We'll request named users be setup within a customer's Entra ID Tenant to do this work if needed, though a customer can deny this request and opt for a request based "just in time" access method instead, which will require the customer to grant Redcentric ACE engineers access every time elevated work is required.

The diagram below illustrates Redcentric's access for some of the methods listed above.

11. Managed Azure Services Appendix

Here we describe in greater detail some of the core elements delivered by Redcentric's Managed Azure services, should more detail be needed on anything not listed here, please ask the team.

11.1. Cost Optimisation & Tooling

Redcentric will provide access to our Billing Analytics Platform which provides customers with a wealth of information on Azure best practices including Cost Management, Right Sizing and Security Advisories. This analytics platform will continually review each deployment and feedback vital information to the management teams. This service can also integrate into the Redcentric Service Desk team triggering and triaging alerts on spend threshold breaches and new advisories.

The Redcentric ACE Azure team will work with the customer to help identify cost optimisations through new architecture, services, incentives, reservations, and best practices to avoid spiraling costs or bill shock.

11.2. Governance Reviews (Scheduled)

The continued governance of the Azure environment is key to success of Public Cloud adoption and ensuring Best Practices are followed and audited. As part of the Govern service, Redcentric will schedule governance reviews covering partly or all of the below areas based on a customer's requirements:

- **Azure Advisor Review:** Work through recommended advice and agree actionable items.
- **Cost Management:** Review of optimisation tools to provide recommendations for controlling spend.
- **Security Centre:** Check compliance with required standards and review current security posture.
- **Identity Management:** Review of management groups, RBAC and identity controls.
- **Policy Reviews:** Check policies are effective and representative of required controls and objectives.
- **Compliance Score Benchmarks:** Outline roadblocks to achieving desired outcome or objective.
- **Remediation Workshops:** Advised assistance or coordination with remediation teams to remove roadblocks.
- **Resource Consistency:** Review tagging and naming to ensure agreed standards are consistent across projects.
- **Deployment Acceleration:** Discuss current deployment approaches and review improvement areas.
- **Operability Improvements:** Keep track of improvement actions and tasks.

11.3. Azure Policy Management & Remediation Assistance (Scheduled)

Azure Policy helps to enforce organisational standards and to assess compliance at-scale. The compliance dashboard provides an aggregated view to evaluate the overall state of the environment. The Redcentric ACE team will work closely with a customers teams via the Govern service to set and achieve realistic, incremental improvements via reports, workshops and remediation guidance or assistance, enabling a customer to achieve their compliance goal benchmarks.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. The Redcentric ACE Azure team will advise and assist with ensure that appropriate Azure policies are deployed and any required change management in-life to meet new requirements business demands and objectives.

As project teams deliver change at increasing velocity, new resources are being launched, changes are constant and numerous Azure service updates are released every day. Therefore, customers Azure environments are subject to constant flux and with new service updates comes new opportunities. Ensuring the initial Governance MVP develops and improves to a matured model is key to success.

The Redcentric ACE makes Governance Easy		
Workshops to baseline configuration	Schedule policy deployment	Workshops to accelerate remediation
Turn on built-in policies or build custom ones for all resources	Apply policies to a Management Group with control across a customers entire organisation	Remediate on existing resources
Real-time policy evaluation and enforcement	Apply multitude policies and aggregate policy state with policy initiative	Auto-remediation on future deployment
Periodic and on-demand compliance evaluation	Exclusion Scope	Trigger alerts when resources are none compliant
Enforcement & Compliance	**Apply Policies at Scale**	**Remediate & Automate**

The Governance Managed Service aims to drive this improvement with monthly reports and in-flight policy changes to adapt the framework as issues and opportunities arise.

11.4. Architecture Guidance, Validation & Modernisation (Scheduled)

Redcentric Azure services provide customers with access to our accredited ACE teams who will provide hands on validation and design guidance for Azure deployments.

As part of the Modernise service, we understand that one of the main requirements of an infrastructure partner is to work closely with customers and external software vendors (where applicable) to help to define the optimal infrastructure and automation options for our customers applications. This will typically be based on several factors:

- The architecture and software used to build the application
- Predicted usage and access patterns of the application, and the anticipated requirement for planned or un-planned scalability
- Criticality of the application - what is the impact of downtime or unavailability?
- Ongoing support requirements post go live.
- Security requisites and any associated regulatory mandates which need to be adhered to (DPA, PCIDSS etc)
- Commercial impact of different environments.

Redcentric have a track record of successfully delivering this level of consultancy, designing, deploying, and managing end-to-end infrastructure projects based on the output of discovery exercises and workshops.

Please note:

- The initial discussion is estimated to take 30 minutes
- Monthly Hours entitlement cannot be rolled over

Our core design principles for Azure mirror Microsoft Frameworks & Best Practices:

- Design for self-healing. In a distributed system, failures happen. Design a customer's application to be self- healing when failures occur.
- Make all things redundant. Build redundancy into each application, to avoid having single points of failure.
- Minimize coordination. Minimize coordination between application services to achieve scalability.
- Design to scale out. Design the application so that it can scale horizontally, adding or removing new instances as demand requires.
- Partition around limits. Use partitioning to work around database, network, and compute limits.
- Design for operations. Design a application so that the operations team has the tools they need.
- Use managed services. When possible, use platform as a service (PaaS) rather than infrastructure as a service (IaaS).
- Use the best data store for the job. Pick the storage technology that is the best fit for a customer's data and how it will be used.
- Design for evolution. All successful applications change over time. An evolutionary design is key for continuous innovation.
- Build for the needs of business. Every design decision must be justified by a business requirement.

11.5. Optimisation Improvements (Scheduled)

A customers cloud investment and operability must be treated as a "first-class" priority and a shared responsibility between the Redcentric ACE teams and the customer development and engineering teams.

Optimisation Improvements will be focused on improving the following areas at both the OS and Infrastructure levels depending on what services have been onboarded:

- Availability
- Capacity
- Performance
- Scalability
- Security
- Recoverability
- Deployment
- Monitoring
- Logging & Metrics

11.6. Backup Management

Redcentric will provide a backup management service to maintain and improve the existing process where required. The service will handle any backup failures via the event/incident management process, and any restore request under the request process.

The following services will be utilised:

- Azure IaaS Instances: Azure Backup

Example Retention Policy:

- Daily Backups – 7 Day Retention
- Weekly Backup Point – 4 Week Retention
- Monthly Backup Point – 12 Months
- Yearly Backup Point – 1 Year

11.7. Database Management (Optional)

The Database Management service is an additional service which lets customers tap the power of a team of experienced DBAs to remove the frustration, cost, and time of managing the day-to-day database maintenance.

Our ACE DBA team is aligned with a customer's business, ensuring that all their databases remain healthy and optimised. The Redcentric ACE DBA team are available to support the following technologies:

- SQL Server

The Database Management service contains database aligned service capability for the following modules:

- Monitoring using specialist DBA tools
- Incident & Event Management (access to DBA team)
- Request Fulfilment (DBA specific tasks)
- Back Up Management using our best practice scripts to offer granular data recovery points
- Patch Management on a quarterly schedule
- Performance Tuning

As part of our Enable+ & Operate services, Redcentric will provide support for Microsoft SQL Server and Azure SQL Server instances, including installation, basic configuration, monitoring, troubleshooting and backups, as illustrated below if applicable to the infrastructure design. Additionally, Redcentric can provide advanced DBA services tailored to each customer's specific needs for an additional fee that extends SQL management even further.

Included in Enable+ & Operate	Managed Database Service
- Best-practice guidance	- General database consultation - Advanced architecture design & monitoring - Partner engagement
- Database setup and configuration - Microsoft SQL Server cluster initial setup - User administration - Security administration - Database health monitoring	- Diagnostics - Data import and export - Microsoft SQL Server mirroring and log shipping - Microsoft SQL Server cluster maintenance/change
- Backup and recovery (limited to full DB restores) - Configuration of Microsoft SQL Server backups (DB and transaction log) - Monitoring/troubleshooting Microsoft SQL backup job failures - Redundancy Configuration	- Customized maintenance plans - Refresh and migrate data between instances and data centers - Advanced restore requests (point-in-time recovery)
- Availability issues in production	- In-depth incident retrospective - SQL health report

For full details, see the dedicated service description.

11.8. MDR & SOC (Optional)

Secure your organisation 24/7 with the threat detection and response capabilities of a leading MDR and SOC provider. There will be a security managed service (Managed Cyber Security Operations Service), supporting threat detection, triage, investigation, incident response, compliance reporting through the collection and analysis of computer-generated alarms from historical data across a variety of sources and this may include the partial or full remediation of an identified threat.

This service provides:

- Security monitoring provided by a UK-based 24/7 Security Operations Centre
- Integrate Additional Resources and Expertise
- Advanced threat hunting
- Security Automation
- Threat Intelligence
- Focus on proactive detection and response to cyber threats

For full details, see the dedicated service description.

11.9. Vulnerability Scanning (Optional)

Redcentric offers the following options for customers to run vulnerability scans:

1. Use the integrated Qualys scanner in MSFT tooling, set it to run, and have a security consultant review the findings once a month.
2. Scan during scheduled maintenance windows using native Microsoft Azure components. Redcentric ACE engineer provides a readout of any common vulnerability and exposures (CVEs).

Note: Remediation of any findings are undertaken in conjunction with customers to minimize any potential impact to the underlying application.

Vulnerability scanning requires the following tooling:

- Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management is a powerful vulnerability assessment solution natively integrated in Defender for Cloud. Our goal is to enable our customers to have one solution for vulnerability assessments (VA) for all their different cloud and hybrid workloads, then have seamless integration to Defender for Cloud using the same tools and user experience. Its vulnerability assessments are automatically populated in the Defender for Cloud portal as recommendations. With Microsoft Defender Vulnerability Management, Defender for Cloud customers will have access to both agent-based and agentless scans.

During on-boarding, the scope of vulnerability scanning and frequency of scans will be established.

Redcentric's in-house offensive security and penetration testing experts will review vulnerability scan findings on a monthly basis to inform remediation and patch management plans.

Customers wishing to opt out of this service at any time should notify Redcentric support.

11.10. Patch Management (Scheduled)

Redcentric provides automated OS patching services for resources within ACE Managed Cloud — Microsoft Azure. Different methodologies are used depending on the resource in question. Although the patching process is automated, customers can opt to select which patches are applied or permit automatic installation. Automated patching ensures maximum protection for resources within the environment.

The key business objective for patching is to ensure that an appropriate and consistent patching policy and process is in place to ensure appropriate and timely updates are identified on a priority basis, with a minimum negative impact on operations.

Where "zero-day" or "critical day" flaws exist, and a patch is required, these are reviewed internally within Redcentric using the same processes and deployed as quickly as possible in communication with the customer.

The patching process typically consists of four phases:

Assessment and Inventory - the purpose of this phase is to accurately record what software components comprise the operational environment, what security threats and vulnerabilities exist, and whether an organisation is prepared to respond to new software updates.

Patch Identification - the purpose of this phase is to identify patches and software updates as they are released, determine whether they are relevant to the organisation and determine whether an update represents a normal or emergency change.

Evaluation, planning and testing - the purpose of this phase is to decide, for any given patch, whether to deploy that patch into the operational environment, to plan how and when that deployment will take place, and to test the software update in a realistic operational environment, to confirm that it does not compromise business-critical systems and applications.

Deployment - the purpose of this phase is to successfully roll out the approved software update into the operational environment whilst minimising impact on system users.

The Redcentric patch/release management service aims to ensure that the supported estate is fully up to date with the latest hotfixes and security updates for mainstream operating systems (and applications where applicable), and that these are appropriately identified, reviewed and tested prior to deployment. This does not always mean that systems will be patched to the latest release, but to the last known stable release. This is conducted as follows:

- Monitoring of relevant third-party vendors/suppliers' security advisories for patch/hotfix recommendations.
- ensuring that all vendor-supported operating systems are at the required patching level indicated by Redcentric.
- The notification of proposed patches to the customer and application within an agreed monthly schedule.
- Planning and acting on the deployment of service packs that can be remotely deployed.
- Undertaking BIOS and firmware updates where it is necessary to address an immediate security threat.
- Ensuring that all updates are appropriately managed through the Change Management Process.

11.11. Static Resources

Redcentric uses maintenance windows to automate activities such as patching. Each environment contains one or more maintenance windows configured for days/times to suit the customer. Each maintenance window performs a specific set of tasks and will apply to resources as scheduled.

Each maintenance window is allocated a patching baseline. This controls the type of patch to deploy (critical, security, etc.) and the age the patch must be before it is approved (e.g., 7 days old). Where redundant architectures allow, an environment will have two maintenance windows spread 5 to 7 days apart with the updates split equally between the windows.

During onboarding, Redcentric will work with the customer to define the specific maintenance activities and time periods.

11.12. Dynamic Auto-Scale Environments

Dynamic environments are not patched in a traditional manner because the individual resources are considered expendable. Redcentric has developed a process to ensure the underlying resource template is patched appropriately. All resources deployed from this template therefore will be fully patched.

Redcentric will work with the customer to determine the appropriate template to use, the patch application rules and the scheduling of the maintenance window(s). During the maintenance window, the template will be regenerated automatically with all applicable patches. Any relevant auto scale groups will be updated to reference the new template and a rebuild of the auto scale group will be triggered.

11.13. IaC Usage & Access

Redcentric uses blueprints to provide readymade best practices and reference architectures using Infrastructure-as-Code.

Over the years of working in Azure, Redcentric has built a catalogue of templated IaC designs that meet Microsoft's "Cloud Adoption Framework" and "Well-Architected" best practice standards.cccccccc These templates are available for customers to accelerate best practice deployments and are built with Bicep. Examples of these include:

- Hub & Spoke Landing Zone
- Security Policies & Controls
- Windows Virtual Desktop
- Healthcare Landing Zone
- Sitecore Deployment
- Complex Azure Networking
- Bastion Services
- and many more

11.14. Azure VM & Operating System Management & Monitoring

The Redcentric Intelligent monitoring solution allows for continuous monitoring of VM's with operating systems and components. The fully pro-active solution ensures that the environment remains optimised and that any issues can be identified, and appropriate action taken prior to the issues becoming business critical.

The monitoring services will be configured to automatically alert Redcentric when any thresholds are breached thus offering a preventative support management service. The monitoring solution also allows for effective remote remedial action to be taken as all administration tasks can be delivered with speed and efficiency. Redcentric will then remediate the Azure components based on the alerts received to ensure the systems always remain optimised.

Monitoring services will be configured to alert Redcentric in-line with the requested SLAs for the supported components within the customer environment. The assessment of what SLA is applicable to the various instances will form part of the initial familiarisation work.

Operating Systems Supported
All Windows and RedHat Linux versions supported by Azure (not including the Core or Nano versions of Windows Server).

Software agents included in the Redcentric Automated Deployment process:
- Anti-virus software
- Exploit prevention software
- Patch management software
- Monitoring software

The Windows server is created from templates created by Redcentric based on Customer requirements. These templates are stored and can be re-used to create similar resources should the Customer require them. Other supporting resources, including a recovery services vault, automation account and other scheduled maintenance jobs will also be created.

If, under exceptional circumstances, a patch causes issues with a Customer application due to an incompatibility with the application, it is the responsibility of the Customer to fix the affected application. If it is not possible for the Customer to fix the application before the patches are scheduled to be applied to the production platform, the Customer may request that patching of those servers is put on hold.

In the situation where the affected servers remain un-patched after their allocated patch window due to incompatibilities with the application, the affected server will be classed as un-managed by Redcentric and the SLA will be voided.

Where critical patches are issued by Microsoft, Redcentric reserves the right to perform emergency patching to servers outside of the scheduled patch windows if required, for example, but not including when patches for security vulnerabilities are issued. All attempts will be made by Redcentric to ensure that the Customer is notified in advance, and that patching of servers is still performed according to the patch group they belong to.

When a Customer requires automated patching to be performed that is not part of the standard OS patch process, they may raise a change request specifying which patches are required by the Microsoft Knowledge Base (KB) identifier. Missing server name or KB identifier will result in the change being rejected. Raising a change will be taken as acknowledgement that the Customer has tested the patches involved, and that they accept all responsibility for any issue that arises. In the event of an issue occurring after installing these patches, the only method of recovery will be to restore from the most recent known-working backup.
Custom patching will be performed during working hours, and may not take place at the same time as the regular scheduled OS patches.

12. Monitoring Tools

Redcentric utilizes numerous tools to deliver Managed services, here we will list the major ones that can be customised to meet a customer's needs:

12.1. Azure Native Tools

Entra IDvisor is a monitoring tool from Microsoft that can scan resource configurations and then provide possible actions to improve resources for high availability, security, performance and cost -- so users can optimize their deployments.

Azure Automation is a tool for admins and developers to automate cloud management tasks using Azure runbooks. It will monitor for issues or unwanted changes in applications or configurations. Azure Automation can also monitor and ensure updates for Windows and Linux workloads on Azure.

Azure Cost Management plus Billing is a tool used to monitor a user's cloud spending. This tool will break down the costs of specific Azure services and resources.

Azure Service Health monitors active service issues and health advisories. Azure users can use this tool to monitor the status of events in their cloud environment and to plan ahead for maintenance.

Azure Network Watcher offers network monitoring for network performance. This tool can provide insights and metrics on Azure Virtual Networks (VNet), VMs and application gateways. Users can make use of this tool to identify network issues, to enable or disable resource logs in an Azure VNet, and to view network metrics.

Azure Resource Health allows users to diagnose and receive support for service problems in Azure, specifically relating to its use of resources. Azure Resource Health also monitors the current and past health of an organization's resources.

12.2. Redcentric Monitoring Tools

Redcentric will provide access to a pre-configured and managed industry leading cloud monitoring tool, that will provide an at-a-glance insight into the performance, availability and resource use for the estates. Typical features attainable include:

**Automatically discover network devices and interfaces**

- Performance monitoring of CPU, memory, temperature, fan and other hardware
- Interface metrics – throughput, packet and error rates, utilization, flaps
- And more – e.g. QoS policies, IP SLA profiles, VPNs, VoIP features,
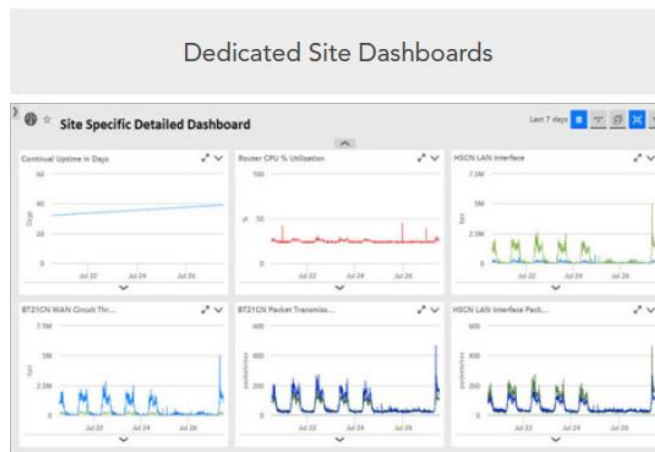- Over 2000 out-of-the-box integrations

With the site monitor feature, customers can track the availability of multi-step transactions and flows, such as registrations and shopping carts on websites and apps. It also provides deep insights into modern service architectures and tracks the performance of containerized applications with user flows, synthetic transactions, and predictive analytics.

It also provides comprehensive coverage of metrics and health monitoring for cloud ecosystems such as AWS and Azure Cloud.

Cloud monitoring features include:

- Troubleshoot quickly with instant and enhanced visibility into cloud resources, log, and application performance, and correlate performance across a customer's entire infrastructure.
- Visualize an entire ecosystem – on-prem, cloud, and microservices – within one platform, streamlining previous workflows that may have leveraged legacy or vendor-agnostic platforms.
- Automatically put the right log events in the context of IT Infrastructure performance giving users the necessary insight to know where and why an event is happening.

Example Meraki Interface   Network Overview

Dedicated Site Dashboards
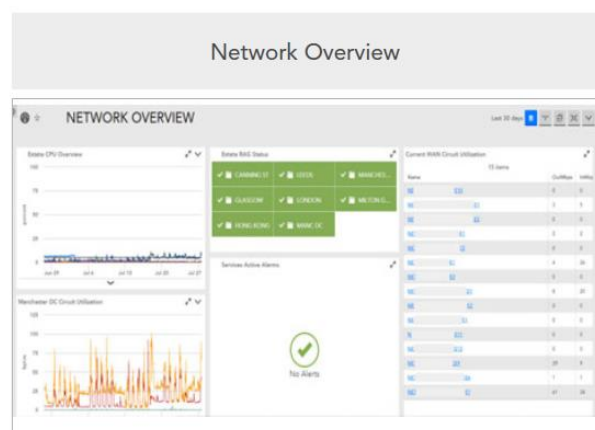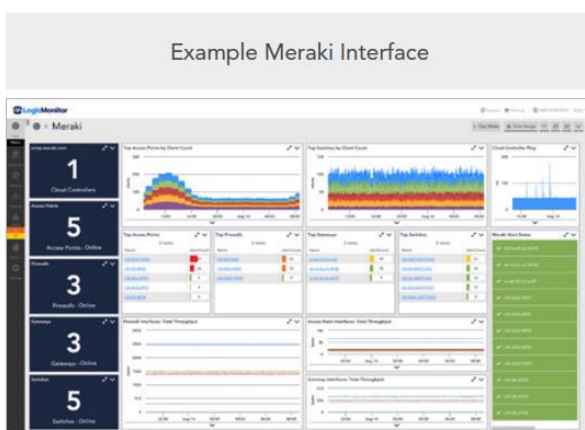
Integrations

Redcentric can provide numerous OS metrics from customer's servers. Track all server-based applications such as databases, mail servers, and web servers. It includes out of the box Logic Modules for monitoring and critical performance metrics to build out dashboards that show the data for the following Application and Database technologies:

Oracle, Redis, Cassandra, MS SQL Server, Postgre SQL, MongoDB, MySQL, Java, NJINX and Apache Tomcat.

It also offers Intelligent Log anomaly detection by correlating relevant logs with metrics in a single platform with out-of-the-box integrations or via any custom log source.

In additional to providing a comprehensive dashboard, logic monitor also support Rest API.

Proactive identification of incidents and faults

Generated alerts are passed directly into our ITSM tool, SMAX which will raise an incident ticket and be supported by an engineer, who will be tasked with verifying the fault to initiate the incident resolution process. Once logged all incidents will be communicated to agreed points of contact and will be governed by the SLA's proposed in the Service Agreements Levels section of this proposal.

Each incident will be reported and available to view anywhere in the world via our customer portal, SMAX. Interactions will be collated and reported via an assigned SDM in monthly service reviews.

70% of all tickets are handled through to completion by this proactive approach. Importantly, our support team are trained to know when to escalate once initial checks have been carried out.

12.3. Data Protection

Data Protection is treated as critical to Redcentric, though Data retention is always the primary customer's responsibility to determine what each policy should be beyond the default policies based on the Cloud Adoption framework. Redcentric ACE teams will work closely with the customer to protect their data and advise on best practices.

Different data types captured:

- **Application monitoring data**, which typically includes data around the performance and functionality of code.
- **Azure resource monitoring data**, which will include data around the operation of an Azure resource.
- **Azure tenant monitoring data**, which gathers data regarding the operation of tenant-level Azure services.
- **Azure subscription monitoring data**, which collects data pertaining to the operation and management of Azure subscriptions.
- **Virtual machine and cloud services data**, which captures system data and logging data on VMs.
- **Application insight data**, which relates to application performance monitoring (APM).
- **Azure Active Directory reporting data**, which collects information on user sign-in activities and system activity.
- **Activity logs**, which collects information on operations performed on resources in a subscription.
- **Network security logs**, which will collect data on traffic flowing through a network.

Metrics and Logging
To seek improvement areas and evidence the rationale it is important that the team has access to a rich set of metrics and logs. The managed service encourages the use of the Azure native service such and Log Analytics and Insights to provide shared information that both teams can use as a single source.

13. Service Support & Availability

13.1. Redcentric Foundations Support

Azure Foundation Support is designed for customers who need minimal day to day support from Redcentric either because they are yet to deploy production services or have considerable experience and resources in house.

Microsoft Advanced Support Escalations

Regardless of whether purchasing Azure infrastructure directly from Microsoft (EA/Direct) or through a Redcentric Cloud Solution Provider (CSP) agreement, Redcentric serves as the sole point of contact for supporting customer's Azure environments. As a part of the Platform Essentials service, if Microsoft ever needs to be contacted for technical escalations, Redcentric will do so on the customer's behalf by leveraging our Microsoft Partner Premier Support agreement.

Foundation Support requires Redcentric to be nominated as your preferred CSP & Partner, allowing Redcentric to provide Business Hours (8x5), Incident Management support, premium issue escalation to Microsoft, plus management of SLA service issues with Microsoft.

Escalations may occur for the following scenarios:

- An Azure subscription service limit increase is required (e.g., number of CPU cores).
- An issue that requires the involvement of a specific Azure product or engineering team to resolve.
- An issue where multiple customers are impacted (e.g., Azure service outages).
- Azure infrastructure SLA credit requests (when infrastructure is purchased through Redcentric CSP).

Priority	Target response time	Target resolution time	Level 1 escalation*	Level 2 escalation
Faults & Technical Query Acknowledgement	30 minutes	Microsoft Delivered	2 hours	3 hours
Remediation Actions Commence	2 hour	Microsoft Delivered	4 hours	6 hours

13.2. Service Desk & ACE Support Request Resolution Targets

For all services above Foundations, the target response and resolution time for the fully managed Azure service includes all the required, modernisation, operations, governance maintenance and reporting activities.

Priority	Target response time	Target resolution time	Level 1 escalation*	Level 2 escalation
Critical/High (P1)	30 minutes	4 hours	2 hours	3 hours
Medium (P2)	1 hour	8 hours	4 hours	6 hours
Low	2 hours	12 business hours	8 business hours	10 business hours
RFI	2 business days	10 business days	8 business days	9 business days

13.3. Request Handling

Requests are typically from customers or are pre-agreed to request service changes. We completely remove the need for our customers to have an in-house administrator. The below table provides an overview of the typically included service requests. Please note any Azure changes which require authorized provisioning of resources will require delegated rights (e.g., storage increases)

Enable & Operate Examples (Platform / Network / OS)

Request	Included
Azure Service Configuration Change	✓
Change/ Add/ Move Azure Storage	✓
Perform Azure Backup	✓
Verify a backup operation	✓
App Gateway Rule Change/ Add/ Delete	✓
Amend Azure VNet Configuration	✓
Azure CSP Subscription Query / Resource Increase	✓
Reboot Azure IaaS VM	✓
Amend Instance Sizes	✓

Note, not a full list.

13.4. Change Enablement

Change Control Process

Changes to a customer's current services will follow the process outlined in the Redcentric Change Management policy.

At a high level, the process of change will follow the below flow:

Typically change requests are initiated from one of the following categories:

- Service Requests
- Incidents
- Problems
- Technology changes
- Business changes
- Customer changes
- Supplier changes

The proposed change will then enter an assessment phase to ensure the change has been fully tested and any impacts to service is understood. Once the assessment is complete the change will be submitted to the Redcentric Change Approval Board for approval. Once approved the change will be scheduled and, if required, communications sent to the agreed parties within the customer once the change is completed, further communications will be sent to advise all customer stake holders.

Normal Changes

The following response times apply to Standard changes. Ad Hoc Changes and Major Application Changes/Releases fall outside the scope of the service and will be managed per request.

Target Response Time	*Implementation Time
16 Redcentric business hours	40 Redcentric business hours

*The implementation time is measured from when the support team have received and validated the Request for Change.

Emergency Changes

The following response times apply to Standard changes. Ad Hoc Changes and Major Application Changes/Releases fall outside the scope of the service and will be managed per request.

Priority	No. Per Month
Emergency change	1

Emergency changes are described as unscheduled or unplanned changes. Typically, emergency changes are driven by immediate and urgent business requirements; for example, updates to site content to mitigate legal action.
The cap on emergency changes does not include changes implemented by Redcentric that form part of the resolution of a service outage or degradation.

13.5. Service Hours Definition

There are 2 levels of Redcentric service hours, defined as follows.

Service Hours Description	Definition
24x7x365	Available 24 hours a day, 7 days a week, 365 days a year.
Redcentric UK business hours (PBH)	09:00 am to 17:00 pm GMT / BST (as applicable) Monday to Friday excluding UK public holidays

13.6. Applicable Service Hours

Service Management Activity	Service Hours
Redcentric Service Desk	24x7x365
Support Request Management	Redcentric UK business hours
Incident Management (P1)	24x7x365
Incident Management (P2 & P3)	Redcentric UK business hours
Problem Management (RCA)	Redcentric UK business hours
Configuration Management	Redcentric UK business hours

The management of support requests (covering requests for information, ticket updates and request for change) will be provided within Redcentric business hours, to ensure the quality of the communication channels.

More specific aspects of service management, such as root cause analysis where the underlying cause of an incident is not yet identified – known as a problem – and the management of change and releases are also carried out within Redcentric business hours to ensure the rigorous and effective delivery of these service elements.

13.7. Redcentric Service Levels

Target availability for the Redcentric services underpinning the **Customer** services.

Service	Target Service Level	Definitions
Redcentric Service Desk	99.90%	Service Desk availability to raise support requests for Customer.

*As all services involved in delivering this rely on the Azure platform and services to some extent, we are reliant on Microsoft to adhere to their own SLAs, some of which are defined below:

Azure Service	SLA
All Azure Platforms and Services	Service Level Agreements (SLA) for Online Services

Any issue that sits with Azure to resolve is not included in any Redcentric SLA calculations.

*Target figure relates to availability of the service platform and excludes outages related to single points of failure, scheduled downtime, or those service elements outside of the Redcentric scope of responsibility.

Platform/infrastructure availability is measured by Redcentric's chosen monitoring and event handling and Redcentric's reporting platform (POM). Redcentric does not include as standard the monitoring of end user perception of availability or performance, which can be affected by the service quality of the ISP or Customer LAN.

Service Availability target is defined as the percentage of time for which the service is available to the users.

$$\text{Service Availability} = \frac{\text{Agreed Service Hours} - \text{Service Downtime Hours}}{\text{Agreed Service Hours}} \times 100\ \%$$

Notes:
All availability targets are to be calculated on a rolling 12-month basis.

Availability calculations will exclude outages where root cause is determined to be outside of the Platform components under Redcentric control.

14. Responsibilities and Accountabilities

High Level Redcentric Responsibilities

Redcentric will provide the following in connection with the Azure platform and managed by Redcentric:

- Creation and configuration of Microsoft tenants and Azure subscriptions on the customer's behalf if required.
- Provisioned access to required tools and portals.
- Migrating customer's data and services as defined in any SOW's.
- All deliverables stated in the scoping matrixes depending on the service level contracted to.
- Feature deployment as agreed-upon during design phases.
- Support tickets created and liaised with Microsoft support when required.

High Level Customer Responsibilities

The customer will:

- Maintain licensing for any software not provided by Redcentric.
- Adhere to the applicable Microsoft terms and conditions.
- Maintain passwords in a secure manner.
- Respond to Redcentric requests in a timely fashion.

RACI Matrix

The following table outlines Redcentric and customer responsibilities using a RACI model.

- Responsible: Do the task
- Accountable: Approve the task
- Consulted: Input provided to the task
- Informed: Notified on task progress or completion

Redcentric Azure RACI

Task	Redcentric	Customer
Standard Activities		
Provide business and technical requirements	C, I	R, A
Create customer proposal, pricing and contract documentation	R, A	C, I
Design review	R, A	C, I
Create Pre-Sales Solution & HLD	R, A	C, I
Final proposal to customer	R, A	C, I
Contract signature	C, I	R, A
Manage implementation activities	R, A	C, I
Build/provision the solution	R, A	C, I
Test and handover	R, A	C, I
Notify the customer of any service-affecting issues or planned maintenance	R, A	C, I
Notify Redcentric of any planned activities that may impact service	A, C, I	R
Resolve incidents and problems	R, A	C, I
Raise service requests and changes	C, I	R, A
Implement service requests and changes	R, A	C, I
Co-Management		
Co-Managed customer created new resource	C, I	R, A
Changes made by the customer that cause issues or alerts, where we have not been made aware	A, C, I	R
Redcentric best endeavours to resolve changes made by the customer that cause issues or alerts, where we have not been made aware	R	A, C, I
Acceptance of any additional charges as a result of changes made by the customer that cause issues or alerts, where we have not been made aware	C, I	R, A
Co-Managed customer request new resource onboarding for Redcentric management	C, I	R, A
Management of resources post onboarding process	R, A	C, I
Account Management And Tooling		
Provide named Account Manager (AM) resource	R, A	C, I
Standard account reporting	R, A	C, I
Identify opportunities for cost and performance optimization	R, A	C, I
Provide opinions and best practices around account architecture, security and resiliency	R, A	C, I
Create a Redcentric account with an owner/contributor role within the customer's subscription to enable Redcentric automation	C, I	R, A
Discovery		
Understand business objectives and current challenges	R, A	C, I
Schedule and conduct a deep-dive discovery session	R, A	C, I
Understand systems SLAs, RTO and PPO requirements	R, A	C, I
Design & Architecture		
Define architecture options to be considered	R, A	C, I
Agree on high-level design (HLD) architecture	C, I	R, A
Generate high-level application and logical diagrams for proposed architecture(s)	R, A	C, I
Generate detailed infrastructure schematics for proposed architecture(s)	R, A	C, I
Create solution design document	R, A	C, I

Task	Redcentric	Customer
Design for a high availability and security-first approach	R, A	C, I
Design for sizing, scalability and performance	R, A	C, I
Governance		
Align with customer key stakeholders	R, A	C, I
Agree on the cadence schedule	C, I	R, A
Provide the budget details and methodology	C, I	R, A
Review the budget methodology	R, A	C, I
Run initial cost optimisation review	R, A	C, I
Review the initial governance best practice and configuration	R, A	C, I
Implement the initial budget and cost optimisation best practices and configuration	R, A	C, I
Agree proposed Budget Settings and Budget Alerts	C, I	R, A
Budget Setting and Budget Alerts	R, A	C, I
Budget Forecasting	R, A	C, I
Cost Analysis and Prediction	R, A	C, I
Cost Optimisation Recommendations	R, A	C, I
Ideal Workload Placement Recommendations	R, A	C, I
Resource Utilization / Performance Reviews	R, A	C, I
Data Storage Location / Retention Reviews	R, A	C, I
Agree on proposed Recommendations and Remediations	C, I	R, A
Defender for Cloud Custom Policies	R, A	C, I
Defender for Cloud Policy Assignment	R, A	C, I
Vulnerability Scanning	R, A	C, I
Agree on Blueprint & Policy Recommendations	C, I	R, A
Blueprint & Policy Definition Creation	R, A	C, I
Blueprint & Policy Definition Assignment	R, A	C, I
Consultative Engagement to Engage Key Stakeholders to Drive Governance Forward	R, A	C, I
Customer key stakeholders to attend workshops for Compliance Score Remediation Assistance	C, I	R, A
Compliance Score Remediation Assistance	R, A	C, I
Compliance measurement for SLO/SLA purposes	R, A	C, I
Hardening Compliance	R, A	C, I
Monthly Spend reporting by usage/service	R, A	C, I
Infrastructure Implementation		
Deployment of Azure infrastructure using the Redcentric ARM template library	R, A	C, I
Configure IaaS components with VM extensions (anti-malware, monitoring and diagnostics)	R, A	C, I
Deployment of images outside of Redcentric Operating Systems Spheres of Support	C, I	R, A
User acceptance testing (UAT) and sign-off environment deployment	C, I	R, A
Configure and test WAN connectivity for ExpressRoute and site-to-site VPN (Redcentric data centres and managed subscriptions)	R, A	C, I
Configure and test WAN connectivity for ExpressRoute and site-to-site VPN (customer data centres and unmanaged subscriptions)	C, I	R, A
Initial governance assistance through deployment of resource groups and implementation of Azure tagging for Redcentric-managed deployments	R, A	C, I

Task	Redcentric	Customer
Implementation of ongoing change management for Azure infrastructure components	R, A	C, I
Network And Access Security Implementation		
Consult on identity access management (IAM) roles and polices	C, I	R, A
Define Network Security Groups and rules requirements	C, I	R, A
Implement Network Security Groups and rules	R, A	C, I
OS user management per Redcentric Spheres of Support	R, A	C, I
Anti-virus installation, configuration and monitoring for Windows VMs	R, A	C, I
Entra ID (Expanded via Modern Workplace 365)		
Initial deployment of Entra ID	R, A	C, I
Configuration, maintenance and administration of Entra ID as needed to provide access for Redcentric engineering teams	R, A	C, I
Configuration, maintenance and administration of Entra ID as needed to provide access for clients or other third-party vendors	C, I	R, A
Configuration of Entra Connect replication service to extend on-premises AD environment to Entra ID	C, I	R, A
Configuration of Active Directory Domain Services (ADDS)	C, I	R, A
Promotion of new domain controller on IaaS VM in Azure	R	A, C, I
Extending domain controller to new IaaS VM in Azure	R	A, C, I
Procurement, allocation and management of Entra ID premium licenses and features (Basic, P1, P2)	C, I	R, A
Monitoring		
Deployment and management of Redcentric standard OMS log analytics monitoring platform	R, A	C, I
Initial deployment of Azure Application Insights workspace	R, A	C, I
Configuration of up to 3 web test availability monitors	R, A	C, I
Configuration and management of Application Insights dashboards and custom event logging and alerting	C, I	R, A
Configuration of Application Insights synthetic transaction URL monitors	C, I	R, A
Configuration of application performance monitoring (APM) services, like Application Insights, New Relic, AppDynamics, etc .	C, I	R, A
Configuration of any custom OMS alerts	C, I	R, A
Ticketing/Alerting		
24x7x365 access to support for Redcentric standard monitoring services, including initial responses, escalations and troubleshooting of incidents within Redcentric response time SLA guarantees	R, A	C, I
Ongoing definition, management and maintenance of Redcentric standard OMS monitoring platform, including the definition of alert triggers, thresholds and remediation instructions	R, A	C, I
Initial response, escalation and troubleshooting of custom alerts on Azure, including non-standard OMS alerts, APM alerts, etc.	C, I	R, A
Backup & Disaster Recovery		
Creation of an Azure Recovery Service Vault (RSV)	R, A	C, I
Creation and management of VM backup policies and schedules to Redcentric standards	R, A	C, I
Monitoring and remediation of backup failures on Redcentric standard backup service	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	R	A, C, I
Installation, configuration and management of Azure file-level backup agents and service	C, I	R, A

Task	Redcentric	Customer
Azure Site Recovery (ASR)		
Design of DR/BCP strategy, including end-to-end environment failover processes, communication strategy, or any related activity for the creation of a disaster recovery or business continuity plan	I	R, A
Design of ASR architecture to Redcentric best-practices for approved workloads from one Azure region to another	R, A	C, I
Configuration of simple ASR Recovery Plan using a single failover group (custom scripting excluded)	R, A	C, I
Configuration of custom ASR Recovery Plan using multiple failover groups and/or custom scripting	C, I	R, A
Configuration of Azure-to-Azure ASR replication services	R, A	C, I
Configuration of ASR replication module in Redcentric monitoring platform	R, A	C, I
Emergency failover using pre-configured ASR Recovery Plan	R	A, C, I
Perform ASR "Test Failover" service once every six months, allowing validation of infrastructure failover orchestration as well as data replication services (application failover testing excluded)	R, A	C, I
Application failover testing following ASR "Test Failover"	C, I	R, A
24x7x365 incident response for ASR replication issues	R, A	C, I
Azure Kubernetes Service (AKS)		
Design and deployment of AKS infrastructure, including configuration of AKS cluster, nodes, node pools, and Azure Container Registry (ACR)	R, A	C, I
Design and deployment of containers, load balancers, static IP addresses or any other service configured via YAML file	C, I	R, A
Implementation of other Kubernetes packages (like Prometheus, Grafana, Helm, Linkerd, fluentd, Envoy, etc .)	C, I	R, A
Configuration of geo-replicated Azure Container Registry	R, A	C, I
Build, automate, update and deploy container images with Azure Container Registry tasks	C, I	R, A
Monitoring and logging for AKS cluster and worker nodes	R, A	C, I
Monitoring and logging for containers, pods and controllers	C, I	R, A
AKS cluster and worker nodes troubleshooting	R, A	C, I
Containers, pods and controllers troubleshooting	C, I	R, A
Integration of AKS with Azure Active Directory or private docker container registry	C, I	R, A
Integration of AKS into a CI/CD pipeline	C, I	R, A
Upgrade an AKS cluster or patch security/kernel updates to worker nodes in AKS	R, A	C, I
Patching		
Installation and configuration of automated OS-level patching via the Azure update management service	R	A, C, I
Installation and configuration of automated OS-level patching via automatic updates within OS	R	A, C, I
Deployment, configuration and management of any other patch management service	C, I	R, A

15. Terms & Conditions

15.1. Microsoft Service Levels

Azure Service Levels are provided by Microsoft, and not by Redcentric. Azure Service Level Agreements which describe Microsoft's uptime guarantees and downtime credit policies are specific for each Azure service. The SLAs for individual Azure services can be accessed here:

https://Azure.microsoft.com/en-gb/support/legal/sla/

Typically the Azure services have an availability target of 99.9% measured on a monthly basis, but please refer to the Microsoft Cloud Agreement and the related documents.

Microsoft's service terms can be accessed: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=11675

15.2. Microsoft Service Credits

The Azure service performance, including uptime and service monitoring, is the responsibility of Microsoft, and Microsoft is responsible for service credits to the extent set out in the Microsoft Cloud Agreement.

Microsoft will pay to Redcentric any service credits that are due in respect of the Customer's Azure service. Redcentric will credit to the Customer any service credits that Redcentric receives from Microsoft in respect of the Customer's Azure service (where such service has been procured through Redcentric as part of Redcentric's MAS Services). These service credits are described below at their current rates, but may be amended by Microsoft from time to time, in which case the amended service credits paid by Microsoft will apply.

16. Service Responsibilities

16.1. Data Security Responsibilities

Redcentric is responsible for security of the hosted infrastructure and for controlling access by Redcentric staff and ensuring that a customer cannot access data or web sites relating to other customers.

Customer is responsible for all data security issues, excluding those pertaining to the control of access by Redcentric's own staff. This includes ensuring user codes and passwords are managed in a secure way and ensuring data is not made publicly available where inappropriate.

Customer is the guardian of data for General Data Protection Regulation (GDPR) purposes and is responsible for ensuring they hold all intellectual property rights to the content of the data.

16.2. Security Vulnerabilities

It has been agreed that if a Security threat is uncovered, and the software or firmware impacted is a component of the Redcentric-managed software and firmware, Redcentric will take the following action,

If there is a patch or mitigation solution available, and Redcentric is confident the resolution can be applied with minimal impact to service, customer's authorize Redcentric to treat the solution as a pre-approved change, in accordance with the terms of the Managed Services Agreement, and apply such patch or mitigation solution within a commercially reasonable time period to preserve the integrity of the Services provided to customers. After such a patch, the service owner, or nominated representative, will be contacted for verification of the next steps, if necessary.

Redcentric reserves the right to carry out any mitigating action to protect other customers and services hosted in Telehouse. In exceptional circumstances, this could include disconnecting the Customer's systems from the Redcentric infrastructure (Virus outbreak, DDoS, etc).

16.3. End of Life (EOL) Services

Where EOL services and hardware are identified Redcentric teams will inform the SDM for the service. EOL services and hardware will be discussed and reviewed as part of regular service review meetings. Where applicable risks associated with EOL services and hardware will be captured on the Risk Register and managed in accordance with Redcentric Risk Management processes

For clarity any remedial work required to manage EOL services and hardware will incur additional project charges and work will be performed under reasonable endeavors within available resources

16.4. Force Majeure Event

Redcentric will endeavor to identify and track all known risks which have a potential material impact on the integrity of their customers services. This will include all known risks to both services in and outside of Redcentric's managed service. These risks will be tracked in the Risk Register which will be managed in accordance with Redcentric Risk Management processes. However,

where an event(s) or circumstance(s) occurs beyond Redcentric's reasonable control which impacts on services managed and/or owned by Redcentric, out of scope charges may be incurred for any necessary remedial action undertaken by the Redcentric support team(s).

16.5. AZURE Shared Responsibility Model

Redcentric follow the Shared Responsibility Model for Azure which is defined on the Microsoft website.

16.6. Service Providers

Redcentric will act as primary support provider of the services herein identified except when trusted third parties are employed who shall assume appropriate service support responsibilities accordingly.

17. Glossary of Terms

Acronym Key

Acronym	Expanded Term
AoC	Attestation of Compliance
APM	Application performance monitoring
CDR	Customer design requirements
CSP	Cloud Service provider
MCSP	Managed Cloud Service provider
CVE	Common vulnerability and exposures
DRaaS	Disaster recovery as a service
IaC	Infrastructure as code
IDS	Intrusion detection services
IPS	Intrusion prevention services
ITIL	Information Technology Infrastructure Library
PCI DSS	Payment Card Industry Data Security Standard
RCA	Root cause analysis
SLA	Service-level agreement
SME	Service management executive
SOC	Security Operation Center
TAM	Technical account manager
WAF	Web application firewall

18. Disclaimer

This information is subject to formal contract and is an indicative and unqualified invitation to treat not capable of acceptance. no contractual relationship shall exist until formal contract documentation has been negotiated and executed by both parties.

Service category	Cloud

Document Control

Title	Redcentric Azure Service Definition
Originator / Author	Warren Ward
Reviewer	Jonathan Kirby, Steve O'Brian, Richard Baldwin, Paul Mardling, Sam Webster
Business Area	Operations/CSG
Review Cycle	Annual (Due every 12 months from initial release V 1.0)

Change Record

Version	Date	Changes	Change Control Reference	Document Status
0.1	08/09/2021	Initial draft for internal review		In Draft
1.0	24/10/2021	Released		Released
1.1	24/05/2022	Updates		Released
2.0	02/12/2022	Drafted moved into template		Released
2.3	15/01/2023	Updates		Released

Document Ownership

Redcentric's Product Manager for Azure is the owner of this document and is therefore responsible for ensuring that this Definition is reviewed in line with the review requirements of Redcentric's ISO9001 Quality Management System.

HEAD OFFICE

Central House

Beckwith Knowle

Harrogate

HG3 1UG

T 0800 983 2522

E sayhello@redcentricplc.com

W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED