



Service description document: Managed service for public cloud

## Contents

|                                                                                                                                                                              |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Your Microsoft certified managed service partner .....                                                                                                                       | 4  |
| Consultative-led approach .....                                                                                                                                              | 4  |
| Secure foundation .....                                                                                                                                                      | 4  |
| Next-generation IT servicing solutions .....                                                                                                                                 | 4  |
| What the service is .....                                                                                                                                                    | 5  |
| Cloud governance .....                                                                                                                                                       | 5  |
| Cloud monitoring and support .....                                                                                                                                           | 5  |
| eir business protect .....                                                                                                                                                   | 5  |
| eir business defender .....                                                                                                                                                  | 5  |
| Cloud optimization .....                                                                                                                                                     | 6  |
| Cloud expert engineering .....                                                                                                                                               | 6  |
| Cloud desktops .....                                                                                                                                                         | 6  |
| Cloud security operations .....                                                                                                                                              | 6  |
| Service selection .....                                                                                                                                                      | 7  |
| Cloud governance (catalogue of services available) .....                                                                                                                     | 8  |
| Cloud monitoring (catalogue of services available) .....                                                                                                                     | 9  |
| eir business protect – Azure Virtual Machine (VM) backup (catalogue of services available) .....                                                                             | 10 |
| eir business protect – Disaster Recovery (DR) (catalogue of services available) .....                                                                                        | 11 |
| eir business protect – Remote file level recovery (catalogue of services available) .....                                                                                    | 12 |
| eir business protect – Office 365 backup (catalogue of services available) .....                                                                                             | 13 |
| eir business protect – Cloud backup repository (catalogue of services available) .....                                                                                       | 14 |
| eir business defender (catalogue of services available) .....                                                                                                                | 15 |
| Cloud optimisation (catalogue of services available) .....                                                                                                                   | 16 |
| Cloud expert engineering (catalogue of services available) .....                                                                                                             | 17 |
| Levels of data backup and restore, and disaster recovery .....                                                                                                               | 18 |
| Azure Virtual Machine (VM) backup: Providing image or disk level restores, file level restores, application consistent backups, and data retention as per agreed policies. . | 18 |
| Onboarding and offboarding support we provide .....                                                                                                                          | 18 |
| After sales support .....                                                                                                                                                    | 18 |
| Continuous assistance .....                                                                                                                                                  | 18 |
| Dedicated expertise .....                                                                                                                                                    | 18 |
| Proactive monitoring .....                                                                                                                                                   | 18 |
| Responsive resolution .....                                                                                                                                                  | 19 |
| Customised support .....                                                                                                                                                     | 19 |
| Collaborative partnership .....                                                                                                                                              | 19 |
| Accessible communication .....                                                                                                                                               | 19 |

|                                       |    |
|---------------------------------------|----|
| Hosting options and locations .....   | 19 |
| Access to data (upon exit) .....      | 19 |
| Security.....                         | 20 |
| Security training and awareness ..... | 20 |
| Physical security .....               | 20 |

## Your Microsoft certified managed service partner

Estimating the true scale of costs against the functionality of your organisation's demands from public cloud can be difficult. The eir business Managed Service for Azure is truly a cloud-era Managed Service that encompasses the complete design, delivery and daily operational support of your Azure environment.

As a Microsoft Expert Azure Managed Service Provider, we pride ourselves on best practice methodologies and deployment tools that drive quick deliverables across our full Managed Service offering which is based on the following core principles:

### Consultative-led approach

The eir business Cloud Advisory Team is built upon dedicated Cloud consultants who provide expertise across a wide range of cloud technologies, including Azure Public Cloud, Private Cloud Solutions and Hybrid deployments such as Azure Stack, PaaS and SaaS services.

### Secure foundation

We'll conduct our Azure Security Audit to optimise security, availability and cost performance on your Azure platform. This provides a strong foundation to the secure operation of your Azure-based solution and enables further expansion in a consistently secure manner.

### Next-generation IT servicing solutions

Our next-generation IT servicing solutions have been developed over decades of excellence in IT Strategy Review, Solution Architecture, Enterprise System Design, Data Migration and Cloud Management allowing you to get the very best in cloud optimisation, monitoring and management.

## Our Microsoft recognised capabilities

Demonstrating our expertise, customer success, growth of investment and technical readiness, we:

- Have achieved all 6 Microsoft Solutions Partner Designations
- Are a Microsoft Azure Expert Managed Service Provider
- Have invested heavily in our Azure capabilities through our team of Azure Solution Architects guided by Microsoft Practice Director and Microsoft MVP Joe Carlyle
- Have successfully developed a mature Azure Managed Service offering which is based on the ITIL framework and backed by ISO20000 and ISO27001 certifications.

## Microsoft Partner Azure Expert MSP



Data & AI  
Azure



Microsoft Cloud



Infrastructure  
Azure



Security

x

## What the service is

Our Managed Azure Cloud service comprises a comprehensive suite of features and capabilities designed to ensure seamless governance, monitoring, protection, optimisation, security operations, and expert engineering support for your Azure environment.

Based on our experience of working with and supporting public sector clients already using the platform, we understand that every organisation has unique needs and requirements. To facilitate customisation and a holistic approach to building a service that works best for your organisation, we offer a comprehensive range of sub-services under the following key managed Azure cloud services:

### Cloud governance

Our cloud governance service includes a robust Cloud Governance framework, featuring:

- A cloud management platform for streamlined management
- Tenant policy governance to enforce policies
- Cloud asset governance for asset management
- Cloud asset tagging
- Cloud governance reporting for regular insights and reviews

### Cloud monitoring and support

Our cloud monitoring and support services will provide you with complete peace of mind and increased visibility across your Azure environment.

Our support includes:

- Installation and configuration support
- Proactive monitoring and alerts
- Azure platform monitoring
- Comprehensive incident management

As part of our cloud monitoring and support services, we will also provide you with access to a customer facing portal which enable you to view:

- Service monitoring
- URL monitoring
- Custom alerts
- Detailed reporting

### eir business protect

Our protect service has been developed to ensure the safety of your data and applications with Azure VM Backup.

This service includes:

- Remote file level backup
- Azure disaster recovery
- Optional Office365 backup for comprehensive protection

### eir business defender

This service provides customers with antivirus management and consultancy on the patching recommendations that windows defender offers clients, as a next generation antivirus solution. This service is an operations function and can be complimented by a SOC service for incident response and vulnerability services required through eir business.

This service includes:

- Antivirus management
- Encryption management
- Vulnerability reviews
- Microsoft patching
- Third party application patching
- Hardware & bios patching
- Base lining

## Cloud optimization

This service provides a continuous cycle of cloud optimisation, helping manage your cloud presence by offering insights into resource reporting and spend optimisation.

This service optimises your cloud usage and costs with features including:

- Cloud cost monitoring
- Untagged asset monitoring
- Resource utilisation monitoring
- Costs visibility and trending
- Rightsizing reporting
- Hybrid benefit assessment
- Refactor recommendations
- Business unit perspective reporting

## Cloud expert engineering

Our team provides expert support throughout your cloud journey, including:

- Project Support
- Change requests handling
- Incident Support
- Cloud Strategy Support

## Cloud desktops

This service provides customers with a secure, stable and scalable virtual desktop environment which can be fully managed through a single self-service control panel. Standardised, pre-configured virtual desktop templates are deployed as needed and charged on a consumption basis. The key functions offered under this service include:

- VDI Desktop
- Networking
- Storage
- Account Management
- AD domain integration
- User Session Management Facility
- Universal device support
- Desktop Template Design

## Cloud security operations

Our cloud security operations service ensured the security of your Azure environment with features such as:

- Identity management (including privileged identity management)
- User lifecycle management
- Roles and permissions management

We also offer Firewall Management services, including:

- Firewall IP Configuration
- Configuration Backups
- Firewall policy and ACL management
- VPN Configuration
- Intrusion Detection and Prevention
- URL Filtering
- Reporting

## Service selection

The tables on the following pages include an itemised overview of our key and sub-services available under our Managed Azure cloud service. This has been developed in order for you to select a stack of services to best suit your requirements. Our team is happy to assist you with any clarifications or questions you may have with relation to service selection.

## Cloud governance (catalogue of services available)

| Service reference | Service function          | Service features                                                                                                                                                                                                                                                                                                                     | Service constraints                                                                                                                                                                         |
|-------------------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MCS01-AZ.1        | Cloud management platform | This sub-service will provide you with access to our centralised cloud management platform Cloudstore. Via the platform you will have the ability to view and manage a wealth of management information for your Azure environment                                                                                                   | This service is limited to available Cloudstore features. Security permission is required for configuration. The platform will be configured on your Azure tenant through Azure Lighthouse. |
| MCS01-AZ.2        | Tenant policy governance  | Policy implementation and governance across your Azure management groups and hierarchies                                                                                                                                                                                                                                             | N/A                                                                                                                                                                                         |
| MCS01-AZ.3        | Cloud asset governance    | Asset inventory and tracking of all Azure assets and configuration items.                                                                                                                                                                                                                                                            | This service is limited to subscriptions and assets being managed by this service.                                                                                                          |
| MCS01-AZ.4        | Cloud asset tagging       | Management of tagging across Azure assets to business unit and application groups. Alerting of untagged assets.                                                                                                                                                                                                                      | All assets must be tagged as part of our on-boarding process for this service.                                                                                                              |
| MCS01-AZ.5        | Cloud governance report   | We will provide a governance report that will contain the following information:<br>1. Data Centre Location/Data Residency<br>2. Deployed Azure Components<br>3. Best Practice Adherence<br>4. Storage Account Review<br>5. Virtual Machine Review<br>6. Containers Review<br>7. Azure Data Platforms Review<br>8. Networking Review | Reports will be based on available data from your subscription.                                                                                                                             |
| MCS01-AZ.6        | Cloud governance tooling  | We use Azure Lighthouse to govern Azure customers at scale and apply policies and blueprints. We supplement Azure Lighthouse with Azure Blueprints, Azure Policies, Azure Resource Graph and VMware CloudHealth.                                                                                                                     | Tooling permissions and configuration deployed as part of our onboarding. eir business approved tools must be used.                                                                         |
| MCS01-AZ.7        | Cloud governance review   | We will allocate one of our Public Cloud Experts to participate in your governance reviews. They will work as a member of your team to review the governance report and support decision making around its recommendations.                                                                                                          | Limited to 1 review per quarter.                                                                                                                                                            |

## Cloud monitoring (catalogue of services available)

| Service reference | Service function               | Service features                                                                                                                 | Service constraints                                                                                                                                                                  |
|-------------------|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MCS02-AZ.1        | Installation and configuration | Alerting based on monitoring policies applied.                                                                                   | Monitoring connectivity (Internet access) must be available and configured.                                                                                                          |
| MCS02-AZ.3        | Monitoring and alerts          | Monitoring of alerts that are raised by your organisation's environment.                                                         | An eir business Managed Service contract is required to action alerts generated within the OS and above, otherwise alerts will only be sent to customers to action.                  |
| MCS02-AZ.4        | Azure platform monitoring      | Monitoring of Azure platform environmental variables and alerting based on incidents or predefined thresholds on Azure services. | Limited to the metrics that are available to the monitoring user assigned to your tenant subscription.                                                                               |
| MCS02-AZ.5        | URL monitoring                 | Monitoring of website or web application.                                                                                        | URLs will be identified during onboarding and eir business must be notified of any new URLs to be added.                                                                             |
| MCS02-AZ.6        | Incident management            | Action the alerts based on your runbook.                                                                                         | Your organisation will be required provide a runbook of L1 basic actions for eir business to follow. Pre-approval must be in place if these actions incur additional resource costs. |
| MCS02-AZ.7        | Service Monitoring             | Monitoring the availability of your platform services.                                                                           | N/A                                                                                                                                                                                  |
| MCS02-AZ.8        | Web Portal Access              | Web portal access to view alert details for devices monitored.                                                                   | N/A                                                                                                                                                                                  |
| MCS02-AZ.9        | Custom Alerts                  | Configuration of custom alerts aligned to customer's requirements                                                                | Configuration of monitoring and alerting is based on available metrics and functionality of the monitoring platform and must be signed off by your organisation.                     |
| MCS02-AZ.10       | Reporting                      | Monthly reporting of the alerts generated, and machines being monitored                                                          | Specific reporting metrics can be agreed upon based on the metrics available.                                                                                                        |

## eir business protect – Azure Virtual Machine (VM) backup (catalogue of services available)

| Service reference | Service function                        | Service features                                                                                                            | Service constraints                                                                                                           |
|-------------------|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| MCS03-AZB.1       | Azure backup management                 |                                                                                                                             | N/A                                                                                                                           |
| MCS03-AZB.2       | Configure file backup                   | Configure file level backups in Azure                                                                                       | N/A                                                                                                                           |
| MCS03-AZB.3       | Modify backup configuration             | Modify configuration based on client request                                                                                | N/A                                                                                                                           |
| MCS03-AZB.4       | Restore virtual machine or virtual disk | Image or disk level restores                                                                                                | Limited to 1 request per server per month                                                                                     |
| MCS03-AZB.5       | File level restore                      | Application/application-file level restore i.e. restore of application item such as exchange email, calendar, SQL database. | Application aware backups require configuration in advance. Limited to 1 per server per month.                                |
| MCS03-AZB.6       | Retention                               | 30-day data retention                                                                                                       | 30-day retention on disk                                                                                                      |
| MCS03-AZB.7       | Backup                                  | Application consistent backup                                                                                               | Application consistent backups require configuration in advance.                                                              |
| MCS03-AZB.8       | Restore                                 | Image level restores                                                                                                        | Limited to 1 request per server per month.                                                                                    |
| MCS03-AZB.9       | Restore                                 | Application/application-file level restore i.e. restore of application item such as exchange email, calendar, SQL database. | Application Aware Backups require configuration in advance. Limited to 1 per server per month.                                |
| MCS03-AZB.10      | Retention                               | Data retention configured per retention policy                                                                              | Short-term retention configures on hot blob.                                                                                  |
| MCS03-AZB.11      | Retention                               | Additional long term disk retention policy as agreed                                                                        | Retention is configured                                                                                                       |
| MCS03-AZB.12      | Encryption                              | Full data encryption on backups                                                                                             | 256bit AES platform level encryption configured by default.                                                                   |
| MCS03-AZB.13      | Storage                                 | Provision of recovery service vaults                                                                                        |                                                                                                                               |
| MCS03-AZB.14      | Replication                             | Configure and manage geo-redundant recovery service vaults for backup replication                                           | Limited to existing customer disk retention policy                                                                            |
| MCS03-AZB.15      | Testing                                 | Quarterly system integrity testing of the Azure backup solution – including full restore of sample image                    | Reports available on request                                                                                                  |
| MCS03-AZB.16      | Testing                                 | Elective, scheduled restore to facilitate customer file level validation of data                                            | 1 test per quarter on request. Testing of customer data integrity to be carried out by customer. Requires advance scheduling. |
| MCS03-AZB.17      | Monitoring                              | 24x7 monitoring and alerting of the azure backup service                                                                    | N/A                                                                                                                           |
| MCS03-AZB.18      | Monitoring                              | 24x7 monitoring and alerting of backup jobs (job success/failure)                                                           | N/A                                                                                                                           |
| MCS03-AZB.19      | Reporting                               | Regular reports on backup status                                                                                            | N/A                                                                                                                           |

## eir business protect – Disaster Recovery (DR) (catalogue of services available)

| Service reference | Service function                            | Service features                                                                                                                                                           | Service constraints                                                                                                                        |
|-------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| MCS03-AZDR.1      | Azure Connectivity Management               | Options to connect client production and DR environments via express route or Site-to-Site VPN                                                                             | N/A                                                                                                                                        |
| MCS03-AZDR.2      | Firewall Replication                        | Syncing of firewall rules to Azure DR firewall                                                                                                                             | Firewall rules to be provided to eir business onboarding and following any subsequent firewall rule changes in the production environment. |
| MCS03-AZDR.3      | External DR Access                          | Managing public access through Azure networking to DR firewall                                                                                                             | Public DNS management is outside the scope of this service, unless fully outlined in advance by the customer in Customer DR Runbook        |
| MCS03-AZDR.4      | DR Configuration Management                 | Configuration of DR Firewalls, DR Networks and DR Replication Jobs, and DR Recovery Plans                                                                                  | Support replication technologies include Azure Site Recovery and Zerto.                                                                    |
| MCS03-AZDR.5      | Server Replication                          | Block level replication                                                                                                                                                    | Limited to replication technology available from the replication and firewall vendors. Zerto is available for Virtual Machines only.       |
| MCS03-AZDR.6      | Data Replication Encryption                 | SSL encrypted for data in transit to Azure                                                                                                                                 | Limited to encryption technology available from the replication and firewall vendors.                                                      |
| MCS03-AZDR.7      | Replication Monitoring & Reporting          | DR Replication Monitoring                                                                                                                                                  | Connectivity Issues, Extended RPO Breaches & Recovery Times.                                                                               |
| MCS03-AZDR.8      | DR Event Management                         | DR invocation and support, standing up of in scope infrastructure in the requested Azure Region & Subscription, configuration of firewalls, networking and load-balancers. | Configuration per agreed process in Customer DR Runbook. Application configuration such as SQL and AD are out of scope of this service.    |
| MCS03-AZDR.9      | Planned DR test                             | 1 assisted planned DR test every 12 months.                                                                                                                                | 1 assisted planned DR test, equating to 16 hours effort per year included. We require 2 weeks' notice for an assisted, planned DR test.    |
| MCS03-AZDR.10     | Additional planned DR test                  | Additional assisted planned DR test, to be requested by the client                                                                                                         | 1 assisted planned DR test, equating to 16 hours effort per year included. We require 2 weeks' notice for an assisted, planned DR test.    |
| MCS03-AZDR.11     | Application recovery and additional support | Application recovery in a DR Test or Live DR event                                                                                                                         | N/A                                                                                                                                        |
| MCS03-AZDR.12     | Assisted failback service                   | Assisted failback service after DR invocation (in a live scenario - not test)                                                                                              | A suitable environment must be available.                                                                                                  |

## eir business protect – Remote file level recovery (catalogue of services available)

| Service reference | Service function | Service features                                                                                                                               | Service constraints and technical requirements                                                                                                                                                                                       |
|-------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MCS03-RFB.1       | Backup           | Remote file level backup                                                                                                                       | N/A                                                                                                                                                                                                                                  |
| MCS03-RFB.2       | Management       | Management of backup solution infrastructure, backup jobs, retention options and backup issue resolution                                       | N/A                                                                                                                                                                                                                                  |
| MCS03-RFB.3       | Deployment       | Installation and configuration of backup software                                                                                              | N/A                                                                                                                                                                                                                                  |
| MCS03-RFB.4       | Restore          | File level restore                                                                                                                             | 1 request per month included in price                                                                                                                                                                                                |
| MCS03-RFB.5       | Disk Retention   | Disk retention policy as agreed                                                                                                                | N/A                                                                                                                                                                                                                                  |
| MCS03-RFB.6       | Archival         | Long term encrypted archival to tape, media management                                                                                         | N/A                                                                                                                                                                                                                                  |
| MCS03-RFB.7       | Encryption       | Full data encryption on backups                                                                                                                | 256bit AES software encryption                                                                                                                                                                                                       |
| MCS03-RFB.8       | Replication      | Offsite replication of backup data to 2nd datacentre within same jurisdiction                                                                  | Limited to existing customer disk retention policy                                                                                                                                                                                   |
| MCS03-RFB.9       | Testing          | Quarterly system integrity testing of the eir business backup solution – including full restore of eir business sample file/image/application. | Reports available on request                                                                                                                                                                                                         |
| MCS03-RFB.10      | Testing          | Elective, scheduled restore to facilitate customer file level validation of data                                                               | 1 test included per quarter on request. eir business is not responsible for performing checks of customer data within restored files. Testing of customer data integrity to be carried out by customer. Requires advance scheduling. |
| MCS03-RFB.11      | Monitoring       | 24x7 Monitoring & Alerting of Backup Infrastructure                                                                                            | N/A                                                                                                                                                                                                                                  |
| MCS03-RFB.12      | Monitoring       | 24x7 Monitoring & Alerting of Backup Service (job success/failure)                                                                             | N/A                                                                                                                                                                                                                                  |

## eir business protect – Office 365 backup (catalogue of services available)

| Service reference | Service function            | Service features                                                                                                     | Service constraints and technical requirements                                                                                                                                                                                                                                                          |
|-------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MCS03-365.1       | Backup                      | Office 365 Backup per user to include: Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams | Limited to 3 backups per day. In order to back up SharePoint, all SharePoint users must be licensed for Office 365 backup                                                                                                                                                                               |
| MCS03-365.2       | Management                  | Management of backup solution infrastructure, backup jobs, retention options and backup issue resolution             | N/A                                                                                                                                                                                                                                                                                                     |
| MCS03-365.3       | Monitoring                  | 24x7 Monitoring & Alerting of the Office 365 backup Infrastructure, including the self-service portal.               | N/A                                                                                                                                                                                                                                                                                                     |
| MCS03-365.4       | Monitoring                  | 24x7 Monitoring & Alerting of Backup Jobs (Success/failure)                                                          | N/A                                                                                                                                                                                                                                                                                                     |
| MCS03-365.5       | Configuration               | Configuration of backup policies based on the customers' requirements                                                | Limited to the scope of the contract                                                                                                                                                                                                                                                                    |
| MCS03-365.6       | Restores request fulfilment | Image level restores                                                                                                 | Limited to 1 supported request per user per month, otherwise chargeable. Unlimited restore requests via the self-service portal.                                                                                                                                                                        |
| MCS03-365.7       | Restore testing             | Elective, scheduled restore of any Office365 object(s)                                                               | 1 test per quarter on request. The restore request is limited to 10 objects or 10GB, whichever is greater. eir business is not responsible for performing checks of customer data within restored files. Testing of customer data integrity to be carried out by customer. Requires advance scheduling. |
| MCS03-365.8       | Retention                   | Office 365 backups are retained for the length of the contract or unlimited retention.                               | An additional 30-day retention will be maintained, to allow for off-boarding, where access will be provided to the Office 365 backup repository                                                                                                                                                         |
| MCS03-365.9       | Encryption                  | Full 256bit AES software encryption on all backups                                                                   | 256bit AES software encryption                                                                                                                                                                                                                                                                          |
| MCS03-365.10      | Data Redundancy             | Redundant across at least 2 data centre locations and a minimum of 3 storage nodes in each data centre.              | N/A                                                                                                                                                                                                                                                                                                     |
| MCS03-365.11      | Reporting                   | Reports of backup status including restore points and retention per user.                                            | Limited to one report per month                                                                                                                                                                                                                                                                         |

## eir business protect – Cloud backup repository (catalogue of services available)

| Service reference | Service function                    | Service features                                                                                                               | Service constraints and technical requirements         |
|-------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| MCS03-OBR.1       | Object Storage Provisioning         | This service provides customers object storage buckets of the required specification                                           | Accessible using the S3 protocol                       |
| MCS03-OBR.2       | GEO Distribution                    | Your data is replicated to 3 Data centre locations in Dublin, Ireland                                                          | IEDP2, IEDP3, IEDP4                                    |
| MCS03-OBR.3       | Object Lock                         | Data immutability is configured at a bucket level, for data that you want to ensure cannot be changed by a user or by malware. | Object lock limited to 30 days                         |
| MCS03-OBR.4       | Management of Storage Fabric        | Maintenance, Upgrades, Hardware failures, Expansion                                                                            | Restricted to approved network vendors for private SAN |
| MCS03-OBR.5       | Storage Monitoring                  | Monitoring of object storage solution, access networks and buckets                                                             | N/A                                                    |
| MCS03-OBR.6       | Capacity and performance management | Management of SAN capacity and operational performance                                                                         | N/A                                                    |
| MCS03-OBR.7       | Self-service web portal             | Customer facility for Object storage management                                                                                | N/A                                                    |

## eir business defender (catalogue of services available)

| Service reference | Service function                 | Service features                                                                                              | Service constraints and technical requirements                                                                 |
|-------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| ICT20.1           | Antivirus Management             | Ensuring definition updates and compliance                                                                    | N/A                                                                                                            |
| ICT20.2           | Encryption management            | Ensuring encryption compliance and updates                                                                    | Encryption must be part of the new laptop process and joiners/leavers process                                  |
| ICT20.3           | Vulnerability Reviews            | Technical Advisor to review impact of latest vulnerabilities based on the outputs of defender recommendations | Bi- Monthly                                                                                                    |
| ICT20.4           | Microsoft Patching               | Maintenance, Upgrades, Hardware failures, Expansion                                                           | Monthly on servers, weekly on laptops                                                                          |
| ICT20.5           | Third Party Application Patching | Monitoring of object storage solution, access networks and buckets                                            | Kaseya must be consumed as product for deployment in a shared service, dedicated service any tools can be used |
| ICT20.6           | Hardware & Bios Patching         | Management of SAN capacity and operational performance                                                        | Deployment software must be in place                                                                           |
| ICT20.7           | Base Lining                      | Day One vulnerability remediation                                                                             | Project to agree and base line all legacy devices for existing vulnerabilities                                 |

## Cloud optimisation (catalogue of services available)

| Service reference | Service function         | Service features                | Service constraints and technical requirements |
|-------------------|--------------------------|---------------------------------|------------------------------------------------|
| MCS05-AZ.1        | Azure Cloud Optimisation | Cloud Cost Monitoring           | N/A                                            |
| MCS05-AZ.2        | Azure Cloud Optimisation | Untagged asset monitoring       | N/A                                            |
| MCS05-AZ.3        | Azure Cloud Optimisation | Resource Utilisation Monitoring | N/A                                            |
| MCS05-AZ.4        | Azure Cloud Optimisation | Costs Visibility & Trending     | N/A                                            |
| MCS05-AZ.5        | Azure Cloud Optimisation | Rightsized Reporting            | N/A                                            |
| MCS05-AZ.6        | Azure Cloud Optimisation | Hybrid Benefit Assessment       | N/A                                            |
| MCS05-AZ.7        | Azure Cloud Optimisation | Refactor recommendations        | N/A                                            |
| MCS05-AZ.8        | Azure Cloud Optimisation | Perspective Reporting           | N/A                                            |

## Cloud expert engineering (catalogue of services available)

| Service reference | Service function         | Service features       | Service constraints and technical requirements |
|-------------------|--------------------------|------------------------|------------------------------------------------|
| MCS06-AZ.1        | Azure Expert Engineering | Project Support        | Time limited per contract                      |
| MCS06-AZ.2        | Azure Expert Engineering | Change requests        | Time limited per contract                      |
| MCS06-AZ.3        | Azure Expert Engineering | Incident Support       | Time limited per contract                      |
| MCS06-AZ.4        | Azure Expert Engineering | Cloud Strategy Support | Time limited per contract                      |

## Levels of data backup and restore, and disaster recovery

Our Managed Azure cloud service offers comprehensive backup and disaster recovery solutions tailored to your needs within the Azure public cloud environment.

These include:

**Azure Virtual Machine (VM) backup:** Providing image or disk level restores, file level restores, application consistent backups, and data retention as per agreed policies.

**Disaster Recovery (DR):** Offering options for Azure connectivity management, firewall replication, external DR access, configuration management, server replication, data replication encryption, monitoring & reporting, DR event management, planned DR tests, application recovery support, and assisted failback services.

**Modern data backup and recovery:** Including backup, office 365 backup, immutable storage, management, deployment, restores, disk retention, archival, encryption, replication, testing, monitoring, alerting and reporting of backup service.

## Onboarding and offboarding support we provide

We ensure a smooth transition onto our Managed Azure cloud service with comprehensive onboarding support. We will allocate an experienced implementation team who will assist with setting up your environment, configuring services, and integrating with your existing systems within the cloud.

Similarly, when it's time to exit our service, we provide offboarding assistance to ensure a seamless transition of your data and operations within the Azure environment in line with our robust exit policy.

## After sales support

Our Managed Azure cloud service is designed to provide you with ongoing, fully managed support following the initial onboarding process. Our dedicated teams are committed to ensuring the success of your deployments within the Azure public cloud environment.

## Continuous assistance

Beyond the initial onboarding, our support teams remain accessible to address any issues, provide guidance, and optimise your Azure deployments for performance, security, and cost-control.

## Dedicated expertise

You'll have access to Microsoft Practice Team who possess in-depth knowledge and experience in managing Azure environments. Whether you encounter technical challenges, require assistance with configurations, or need strategic advice, our experts are here to help.

## Proactive monitoring

We proactively monitor your Azure resources to identify and address potential issues before they impact your operations. Our proactive approach helps minimize disruptions and ensures the reliability of your services within Azure.

## Responsive resolution

In the event of any issues or incidents, our support teams provide rapid response and resolution, ensuring minimal downtime and maximum uptime for your Azure deployments. You can rely on us to promptly address any concerns and keep your operations running smoothly.

## Customised support

We understand that every organization's needs are unique. That's why we offer personalised support tailored to your specific requirements within the Azure environment. Whether you need assistance with deployments, optimisations, or troubleshooting, our support teams are ready to assist you.

## Collaborative partnership

We view our relationship with you as a partnership aimed at achieving your business goals. Our teams work closely with you to understand your objectives, address your challenges, and continuously improve the performance and value of your Azure deployments.

## Accessible communication

Communication is key to effective support. We operate a 24/7 service desk and provide various channels for you to reach out to us, including email, phone, and ticketing systems. Our responsive communication ensures that you receive timely assistance whenever you need it.

## Hosting options and locations

Our Managed Azure cloud service offers flexibility in deploying and managing your workloads within the Azure public cloud. Leveraging Azure's global network of data centres, we can deploy your resources in locations that best meet your performance, compliance, and data residency requirements within the Azure environment.

Second line backup services such as cloud vault/S3 immutable storage can be hosted within our own tier 3 data centres located in the UK and Ireland or configured in the Azure region of your choice, ensuring reliability, security, and compliance with diverse regulatory requirements. These tier 3 data centres are strategically located and ISO27001 certified to meet the highest standards of security protocols and practices.

## Access to data (upon exit)

We prioritise transparency, compliance, and client satisfaction to ensure a seamless and satisfactory offboarding experience.

Access to data upon exit is a critical aspect of our offboarding support services. We understand the importance of safeguarding your data integrity, regulatory compliance, and operational continuity throughout the transition process.

Our approach encompasses careful planning, secure data extraction and migration, thorough resource decommissioning, contractual closure, knowledge transfer.

## Security

Although your services will be hosted in the Azure environment, eir business follows best practice security principles. Based on **20 years'** experience of working closely with public sector clients, we understand that public sector organisations find themselves in an increasingly complex cyber threat environment due to internal and external risks, such as hacks, cyber-attacks and data leaks.

As a SOC provider, with experience in designing, deploying and operating SOC services in critical environments, we have the appropriate skills, knowledge and capability to ensure that your environment and systems are continually protected from security risks. We follow security best practices in the design and deployment of all systems involved in our service provision. For continued reliance, this includes the provision of a robust Threat Management and Incident Response Plan with frequent simulation testing, reviews and improvement activities.

Our robust Information Security Management System (ISMS) is accredited to **ISO27001** Information Security Management Standards and is aligned with NIST Cyber Security Framework. Our ISMS complies with and exceeds the guidance of the NCSC. We also hold a Cyber Essentials accreditation.

### Security training and awareness

Information Security training is mandatory for staff and provided through our online tool, Meta Compliance.

Our training requirements are governed by our Competence and a dedicated Training Coordinator, who is supported by the Quality and Compliance Team and Security Operations Centre to ensure security skills/ training and competencies, are managed throughout the business.

Training is a continuous process provided through technical partners, workshops, awareness and risk-based training.

We also host regular forums to highlight:

- Lessons learned and actions for continuous improvement
- Emerging IT industry security threats/challenges
- Legislative compliance/policy updates

### Physical security

All physical locations used in the hosting of our systems or services are protected with the highest levels of physical security. Meeting public sector requirements, we only use Tier 3 data centres which maintain:

- Full-time on-site security staff
- ID per access-list requirements
- Mantrap-controlled access (to prevent tailgating)
- External and internal alarms and CC-TV security monitoring

Our systems are hosted in private locked rooms, ensuring only authorised staff can access these systems. All access must be pre-approved and is logged for auditing by the data centre and eir business.

Our offices are protected by swipe card access, manned reception areas, and are monitored by 24-hour security. Additional internal swipe card access is designated for specific areas within the building, ensuring minimum physical access is granted based on job roles.