Appendix 1:
Part B- Requirements and Specifications

1 Introduction

Tenderers must address each of the issues and requirements in this part of the RFT and submit a detailed description in each case which demonstrates how these issues and requirements will be dealt with / met and their approach to the proposed delivery of the Services. A mere affirmative statement by the Tenderer that it can/will do so or a reiteration of the tender requirements is NOT sufficient in this regard.

2 Background and Context

The Central Statistics Office ("CSO") was established in 1949 as Ireland's national statistical office. Its status was formalised in legislation with the enactment of the Statistics Act, 1993. It is currently on three main sites, i.e., Skehard Road, Cork; Ardee Road, Rathmines, Dublin 6; and Swords Business Campus, Swords, Co. Dublin.

The mandate of the CSO, as set out in that Act, is the collection, compilation, extraction and dissemination for statistical purposes of information relating to economic, social and general activities and conditions in the State. It is also responsible for coordinating official statistics produced by other public authorities and for developing the statistical potential of administrative records. The CSO places a very high value on its obligation to respect statistical confidentiality and has put an extensive system of safeguards in place to protect the data which the CSO receives. Confidentiality is one of its core values.

The CSO's 2030 long-term strategy highlights the need to continually modernise by being a provider, innovator, enabler and leader in delivering independent insights for all. Harnessing the right technology is identified as a key challenge for the organisation. One of the enablers to harnessing the right technology for the CSO is cloud computing.

The CSO has implemented a cloud computing strategy to provision and manage cloud-based compute and storage resources and has established an operational public cloud environment aligned with Irish Government policy. Core systems and workloads are currently operating within this environment, supported by a hybrid cloud model. The existing environment includes established landing zone capabilities, cloud platform services and business-critical workloads requiring ongoing operational management and support.

The CSO now seeks to further mature, operate and maintain its existing public cloud environment through the provision of Managed Services. The CSO requires an MSP to manage and support the operational cloud environment on an end-to-end basis, from the existing landing zone and core platform services through to the in-scope workloads and applications, in accordance with CSO-defined governance, security and approval controls.

The focus of this procurement is exclusively on the ongoing management, optimisation, security and support of the existing AWS cloud environment and associated workloads (including new workloads that may be delivered over the course of the Agreement).

The CSO shall retain responsibility for cloud financial governance and FinOps. The CSO will operate a cloud observability tool to provide a consolidated view of cloud assets and activity across relevant environments. The MSP shall operate within this model and shall receive, review and manage relevant operational alerts arising from that tool as part of the managed service.

Further information on the CSO is available at https://www.cso.ie.

3 The Services Required

As Ireland's national statistical agency, the Central Statistics Office (CSO) operates critical digital services that support the collection, analysis and dissemination of official statistics. The CSO operates an established and secure public cloud environment hosted on Amazon Web Services (AWS), supporting business-critical systems including survey and Census-related workloads.

The CSO recognises the importance of ensuring the continued secure, reliable and cost-effective operation of this environment in support of its statutory and operational responsibilities. Accordingly, the CSO seeks to engage a Managed Service Provider (MSP) to manage, operate and maintain its existing public cloud environment.

The scope of this procurement relates exclusively to the ongoing operational management, optimisation, security and support of the current cloud environment and associated workloads. It does not include the procurement, selection, redesign or build of a new hyperscaler platform.

Operating Principles and Assumptions

The following principles shall apply throughout the Contract:

- The AWS environment, including all accounts, configurations, data and workloads, is owned by and registered in the name of the CSO.
- The MSP shall be granted controlled, role-based access solely for the purpose of delivering the contracted services.
- The MSP shall not own, resell, rebrand or commercially bundle any part of the CSO's AWS environment.
- Strategic cloud governance, architectural authority and FinOps ownership shall remain the responsibility of the CSO.
- The MSP shall operate strictly within CSO-defined policies, standards and approval processes.
- AWS shall remain the CSO's hyperscale cloud provider for the duration of the Contract.
- The CSO will procure, own and operate an independent cloud observability tool for the monitoring of relevant cloud assets, services and events.
- The MSP shall operate in conjunction with that tool and shall receive, review, triage and manage relevant alerts arising from it, together with any associated operational actions, investigations, escalations and service response activities required in connection with the managed service.

Service Delivery Expectations

The successful tenderer shall be required to:

- Provide ongoing operational management, monitoring and support of the CSO's existing public cloud environment to ensure performance, security, resilience and cost efficiency.
- Support the operation, optimisation and continuous improvement of CSO workloads deployed within the cloud environment, including capacity, performance and cost optimisation activities.

- Provide operational management and support for the existing landing zone, core platform services, in-scope workloads and applications within the managed cloud environment.
- Collaborate with the CSO to ensure the cloud environment continues to meet business, technical, security and regulatory requirements.
- Provide appropriate training, documentation and knowledge transfer to the CSO Cloud Team to support effective oversight and informed decision-making.
- Deliver the managed services for the duration of the contract term, comprising an initial period of three (3) years with the option of up to two (2) one-year extensions at the sole discretion of the CSO.
-

Service Levels

The service levels, response targets, reporting requirements and enhanced support arrangements applicable to the managed service are set out in the relevant sections of this Appendix, including Service Desk and Operational Support, Incident / Major Incident Management, Availability / Capacity / Resilience Management and Reporting / Governance.

Clarification of Ownership and Authority

For the avoidance of doubt:

- The CSO shall retain ownership of the public cloud environment and any configurations, documentation or artefacts developed by the MSP in the course of providing the Services.
- The CSO shall retain direct contractual arrangements with the cloud service provider(s).
- The MSP shall operate within the constraints of existing cloud provider agreements and in accordance with the CSO's contractual, security, data protection and regulatory requirements.
- Responsibility for FinOps, cloud financial governance, budgetary control and the CSO's cloud observability capability shall remain solely with the CSO. The MSP shall not assume ownership of any such functions.

4 The Current Environment

The CSO operates a multi-account AWS environment designed to host statistical applications and data dissemination services. To provide a well-architected, secure, and standardized foundation for deploying statistical workloads, supporting data collection and public data dissemination. The environment is managed under an AWS Landing Zone Accelerator **(LZA)** with an AWS Organisation configured. It utilizes central ingress and egress with a central firewall and a transit gateway for connectivity.

Production, **UAT**, and **Development** environments are used for each of our applications:

- **PxStat:** Open data dissemination platform.
- **Blaise:** Household survey data collection.
- **Census Recruitment & Field management:** Support for Census field staff recruitment and geographical statistical visualization.
- **Census Hub:** Eurostat application hosted
- **Virtual Data Rooms (VDR):** Secure data access for external researchers.
- **Colectica:** Metadata management platform.
- **Census.ie:** The census website.

The environment maintains site-to-site VPNs between the AWS environment and the CSO LAN.

4.1 Existing Landing Zone

The CSO operates under an AWS Landing zone accelerator (LZA) (https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/)

This is a **well-architected, secure, and standardized multi-account environment** that serves as the foundation for deploying our workloads into the cloud.

Our landing zone is the “cloud foundation” before real workloads are deployed. It ensures:

- Security by design
- Compliance with internal and external requirements
- Separation of environments (dev / test / prod)
- Controlled access using IAM and policies
- Centralized observability (logs, monitoring, alerts)*
- Cost management and accountability

***Integrated with Datadog.**
Datadog is the CSO's main tool for infrastructure and application performance monitoring. It is used exclusively for metrics, dashboards, and real-time alerting. It is not used for log

ingestion or log management. All system and application logs are retained within the relevant AWS account.

Our LZA is integrated into ENTRA ID for Single Sign On (SSO) and AWS accounts and roles are tied to these groups with no individual accounts provisioned against AWS accounts. All access management is done via ENTRA ID for CSO staff access with the following groups - **Developer**, **PowerUser**, and **Read-Only** per application per environment. Entra uses **Privileged Identity Management (PIM)**, meaning access is granted for a set duration rather than being permanent; users are removed from groups automatically upon expiration.

Our landing zone is made up of the following central accounts:

- Root Account
- Audit Account
- DevOps Automation
- LogArchive
- Platform Automation
- Shared Networks
- Backup Account

As part of our LZA we operate with a central ingress and egress access point with a central firewall. In addition, there are site-to-site VPNs between our LAN and other environments.

Our infrastructure is deployed via IaC in the form of cloud formation templates (see more below).

4.2 Existing In-Scope Workloads

4.2.1 PxStat

Background
PxStat is a data dissemination management system for publishing statistics in Open Data formats. It is especially designed for National Statistical Institutes and Statistical Organisations, and was developed by the CSO (Central Statistics Office, Ireland) with the support of the PC-Axis Reference Group and the collaboration of the Open Source community.

The system is powered by a lightweight engine and provides a modern, responsive and efficient Web Interface and Web Services (API) for managing and disseminating statistics. End-Users can do the following:

- Run extensive meta-data searches.
- Filter results
- Pivot results
- Explore data by "slicing and dicing"
- Export results to different formats
- Plot interactive charts

- Visualise data over interactive geo-maps
- Share results
- Automate their processes by reading data via API queries.

The outputs also follow the **Open Data** recommendations by providing access to multiple data formats (JSON-Stat, PX, XLSX, CSV) and is ready to enable RDF and LOD (Linked Open Data) to reach *"5 Star Linked Open Data"*.

PxStat also empowers data owners to:

- Manage the publication of their data through a workflow to identify and prevent
- issues before going live
- Track and schedule releases to implement embargo policies
- Compare data and meta-data across releases over time
- Monitor the consumption of data via analytical tools.

See the PxStat GitHub repository for further details here:
https://github.com/CSOIreland/PxStat.

Key Stakeholders
Internal Stakeholders are as follows:

- Statistical Business Areas: responsible for creating and maintain datasets and the entire eco-system.
- Digital Communications division: responsible for creating and maintain datasets and the entire eco-system.
- Cloud and Cybersecurity divisions: responsible for looking after the relative competencies.
- Technology Dissemination: responsible for designing, developing, system testing and maintaining the PxStat project.

External Stakeholders are as follows:

- Government Departments responsible for publishing statistics: responsible for creating and maintain datasets and the entire eco-system
- Open-Source community (i.e. NISRA, PX Community): responsible for contributing to code enhancements and fixes.
- General public: consumes the data.

Existing Configuration

- Single page application using a static website
- Implemented by CSO in Ireland (at data.cso.ie) and NISRA in Northern Ireland (at data.nisra.gov.uk)
- Back-end multiple APIs in a monolith configuration
- Only SQL and NO-SQL data is stored.
- APIs are called from the client browser via javascript functions
- CORS configuration to ensure some APIs are only called via the client
- Some APIs may be called from outside the client without authentication

- CSO users authenticate either via Active Directory (windows identity passed to the application)/Entra or via a bespoke 2FA authentication mechanism
- Non-CSO users may optionally authenticate via Firebase

Background Services
None

Interfaces
None

Existing Environment
- Server Application developed in .Net 8/10 Also uses JS, CSS, and HTML5.
- Windows Server 2019 and Linux used for all servers
- AWS RDS SQL Server 2022 database
- Memcached caching
- AWS SES for email functions
- Typically, 300,000 to 350,000 hits per day
- 15,000 individual datasets hosted with 2.5 billion datapoints

Architecture Diagram

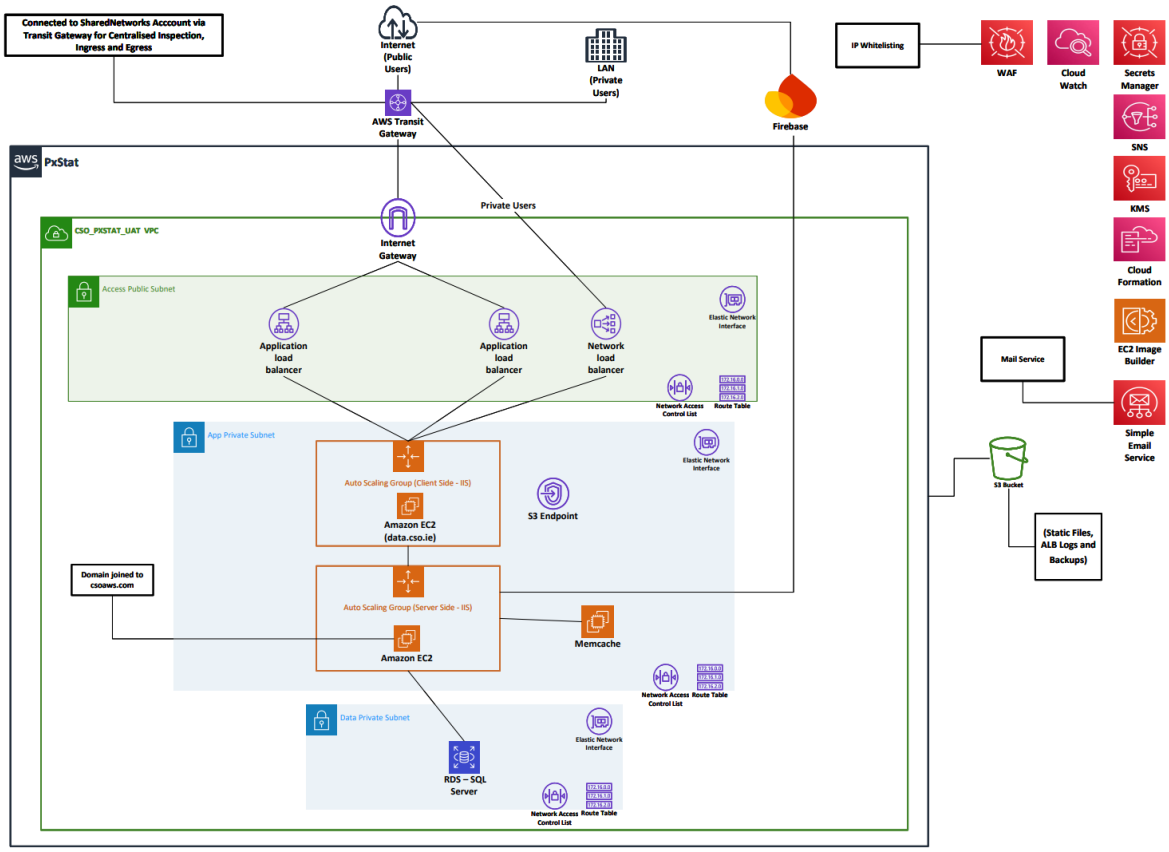

Figure 1PxStat Architecture Diagram

4.2.2 Blaise

Background

Household Surveys are carried out the by the CSO on a continual basis using Blaise technology. The household survey information that is collected is absolutely vital to planning for the present and future needs of everyone in Ireland. The statistics compiled enables the CSO to measure our country's progress on important social and economic issues, such as employment, poverty, childcare, health and crime. Blaise allows surveys to be collected using three modes, computer assisted personal interviews (CAPI), computer assisted telephone interview (CATI) and computer assisted web interviews (CAWI) or online surveys.

In relation to the computer assisted personal interviews, the CSO has a field staff of 10 field coordinators and 130 interviewers who conduct household surveys throughout every county in Ireland every week of the year. For telephone interviews, there is also a call centre who is contracted by the CSO to complete surveys over the phone. The field staff interviews about 1,450 households nationwide every week, using Blaise, a Computer Assisted Personal Interview (CAPI) package, on tablet computers. On the other hand, the call centre completes about 450 Computer Assisted Telephone Interviews per week.

The tablet device provides the cases and questionnaires to the interviewers in the field. On completion of the questionnaires, the devices are individually synched with the CSO via the 2 webservers in AWS. Synchronisation is done at the interviewer location. The field staff may, as is required, schedule meetings with householders and record these events in Blaise Case Management Application (CMA) all of which are sent back to the CSO. These transactions could in any given week amount to around 3,000 pieces of information sent or received by the CSO via this application.

Both the call centre and online surveys are completed on devices and data then securely transferred to CSO using SSL and TLS protocols to ensure secure encrypted transfer of data. When survey details are sent back into the CSO, there are two streams. The survey data is used by CSO Statisticians to analyse and report on the survey data. Survey details are used by the Field Admin Users to manage the completion of surveys by their team.

Key Stakeholders

Internal Stakeholders are as follows:

- Interviewers: responsible for completing the household surveys onsite on HP or other tablets.
- CSO Statisticians: responsible for analysing survey data collected.
- Field Admin Users: responsible for scheduling and managing the completion of
- surveys by interviewers and the call centre.

External Stakeholders are as follows:

- Call Centre: responsible completing the household surveys via phone calls.
- The call centre is an outsourced third party who could be changed from time to time.
- Members of the public who participate in CSO online surveys.

Existing Configuration

Blaise has three environments:

- Production
- UAT

- Development

All three environments work in a similar manner:

- The external facing element of the Blaise systems are implemented in AWS.
- All databases and backend servers are in CSO.

Background Services

Synchronisation of the databases and management of the surveys.

Interfaces

None.

Existing Environments

- Server Application developed from Statistics Netherland
- Windows Server 2019 IIS

Architecture Diagram

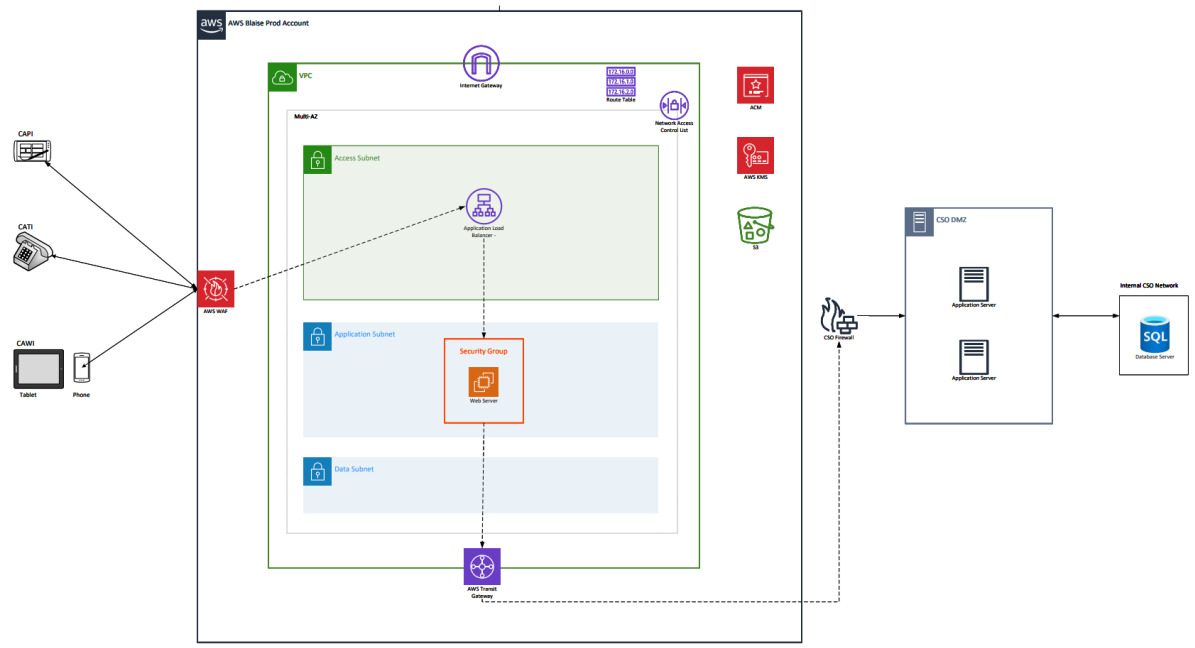

Figure 2 Blaise Architecture Diagram

4.2.3 Census Recruitment

Background

Two core web applications used for Census field staff recruitment. The applications are CSO developed and are running in IIS and .net8/10. The purpose of these applications is to support the next major Census recruitment cycle starting in April 2026 and the ongoing management of the field force once recruited.

Key Stakeholders

Internal Stakeholders are CSO Internal Staff and Field Staff responsible for:

- Review submitted applications
- Candidate shortlisting
- Interview scheduling and management
- Verify uploaded documentation
- Nightly Garda Vetting file generation
- Bulk emailing facility
- Assign successful candidates to Census areas
- Mass Hire/Mass Exit file generation for NSSO
- Manage probation and leave
- View reports for all stages of the recruitment process

External Stakeholders are the General Public who:

- Register for Census roles (Senior Manager (CLO/CRS), Census Field Supervisor (CFS), Census Field Support Officer (FSO)
- Submit applications and required documentation
- Complete onboarding and induction steps

Existing Configuration

Census Online Recruitment Application (Public-Facing) Enables members of the public to:

- Register for Census roles (Senior Manager (CLO/CRS), Census Field Supervisor (CFS), Census Field Support Officer (FSO)
- Submit applications and required documentation
- Complete onboarding and induction steps
- Tech stack: .NET 8/10, SQL Server 2019, jQuery, HTML, CSS.

Census Field Recruitment Management System (Back-Office) Used by internal staff, and field staff to:

- Review submitted applications
- Candidate shortlisting
- Interview scheduling and management
- Verify uploaded documentation
- Nightly Garda Vetting file generation
- Bulk emailing facility
- Assign successful candidates to Census areas
- Mass Hire/Mass Exit file generation for NSSO
- Manage probation and leave
- View reports for all stages of the recruitment process

Authentication:

- Internal staff: via SSO to Entra ID
- Recruitment System: via local login

Background Services

None

Interfaces

None

Existing Environment

- 2 CloudFront distributions, one for internal staff and one for the public
- AWS S3 hosted websites
- 2 ALBs, 1 for internal and 1 for public
- EC2 Instances Windows Server 2019 / IIS within an Auto Scaling Group (ASG)
- AWS RDS SQL Server 2019 database for all environments
- Memcached for caching
- AWS SES for email functions via our Shared Networks account on AWS
- EKS Cluster for Clam-AV Pod for virus detection on file uploads
- S3 for temporary file storage of Garda vetting / payroll files
- FSx for Garda Vetting & Payroll files storage / sharing connected to CSO LAN via VPN
- SMS via 3rd party integration

URLS

- Recruitment.census.ie
- Fieldmanagement.census.ie

Architecture Diagram

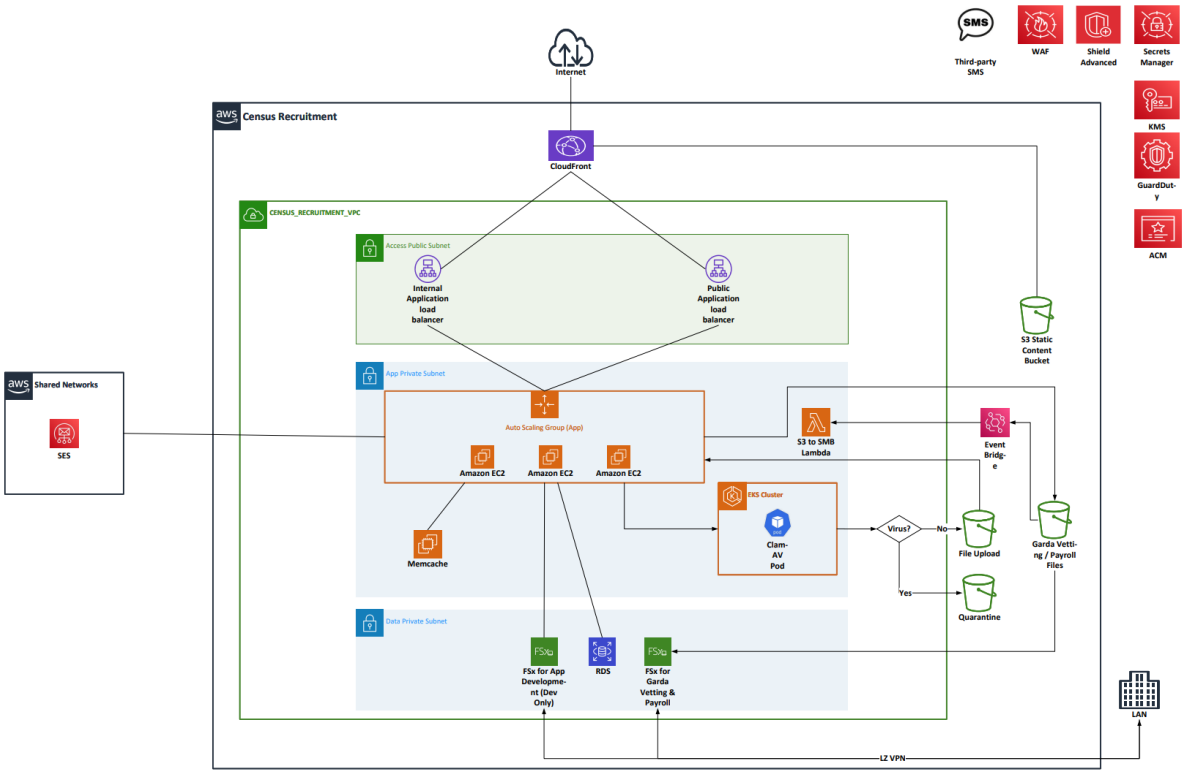

Figure 3 Census Recruitment Architecture Diagram

4.2.4 Census.ie

Background
The census.ie website is of significant, strategic importance to the CSO as it enables the digital online return of Census forms, by the public, to cater for the expectation that approximately 80% of households will submit their Census forms online. Census.ie will form part of the CSO's Digital Census Programme. The site will be used in both phases of the Census 2027 Campaign. It will initially be used in the three recruitment processes to provide information on the available positions and to enable applicants to link to the application form (Census Recruitment). Following the recruitment phase, it will be used to provide the public with relevant information and updates about the Census. It will be used to link the public to the portal where they will complete and submit their online Census form, whilst also enabling people to make contact with the CSO and/or request a Census paper form.

It will have the following features:
- Knowledge Base: a search page connected to a database of Census information
- Chatbot: to assist people with any queries they might have
- Webform: online form used to contact CSO to request a paper Census form/large print Census form or to make enquiries

Key Stakeholders
Internal stakeholders are:
- CSO Census Division – responsible for data collection, processing and publication
- Cloud & Cybersecurity Division – responsible for looking after the relative competencies.

External Stakeholders are:
- General Public – self-service census completion and indirectly, recruitment
- Fusio – design, development and maintenance of site

Background Services
None

Interfaces
None

Existing Environment
- CloudFront Distribution protected by AWS WAF
- AWS S3 hosted website bucket serving static web contents
- AWS CodeCommit and Application Deployment Pipeline for environment releases
- AWS Systems Manager Parameter Store and YAML file for configuration management
- Amazon GuardDuty (S3 Malware Scan) and Amazon EventBridge for automated threat detection on incoming files
- AWS Lambda Function for processing and routing threat-free files
- Multiple S3 staging and repository buckets
- InspectorScan Pipeline with a Manual Approval Gate for artifact validation
- AWS Shield, Certificate Manager, and Key Management Service (KMS) for data protection and encryption

- Cross-account S3 Bucket Sync to a dedicated S3 Backup Account within a CSO Backup AWS environment

URLS

- https://census.ie/

Architecture Diagram

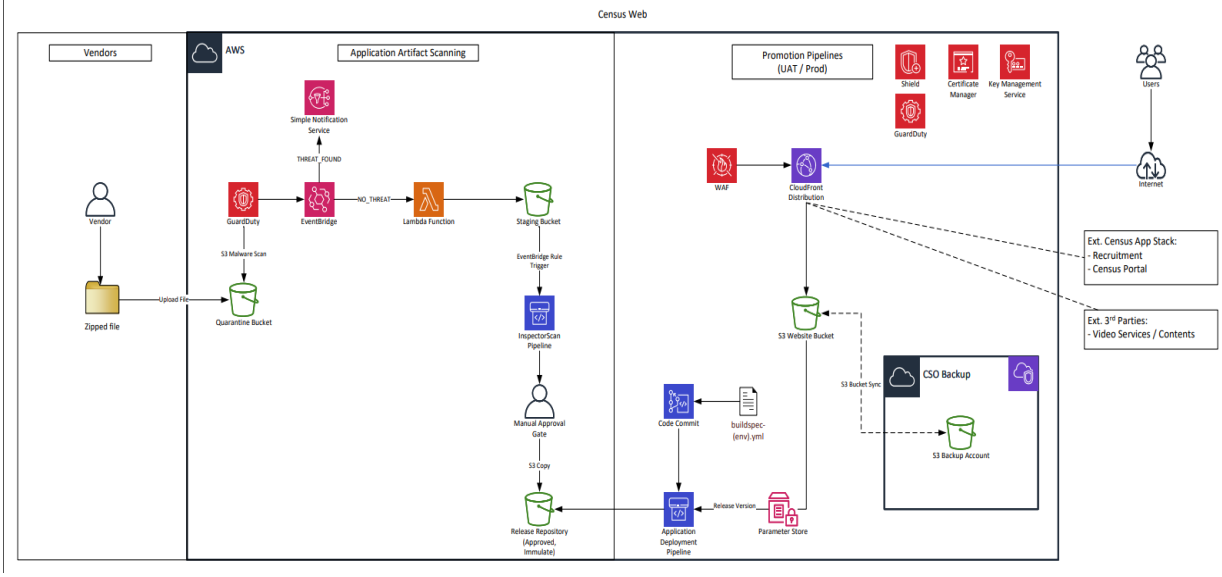

Figure 4 Census.ie Architecture Diagram

4.2.5 Census Hub

Background

Census 2022 and 2016 datasets have been combined with Tailte Éireann's official boundary data as part of a collaborative project between the Central Statistics Office (CSO) and TÉ to link geography and statistics.

Small Area Population Statistics (SAPS) are Census statistics produced by the Central Statistics Office (CSO) for a range of geographical levels, from Administrative Counties to Census Small Areas at the neighbourhood level.

Almost 800 variables across 15 themes can be combined on maps to make powerful visualisations for statistical and statutory boundaries. The data can be visualised here on colour-coded thematic maps. The data is also available through APIs and for download in a variety of formats.

Census Hub is an IIS Server with Eurostat nsiws installed, serving multiple non-critical websites.

Key Stakeholders

Internal Stakeholders are:

- CSO Census Division – responsible for data collection, processing and publication
- Cloud & Cybersecurity Division – responsible for looking after the relative competencies.
- CSO Application development teams – managing application

External Stakeholders are:

- Tailte Éireann (TÉ) – co-developer, provides boundary and geospatial data
- Civil and Public Service organisations conducting statistical analysis
- Businesses & Private Sector – market research, site selection, demographic analysis
- Researchers & Academia – socio-economic and population studies
- General Public – self-service data exploration

Background Services

None

Interfaces

None

Public URL

- https://ec.europa.eu/CensusHub/selectHyperCube?qhc=false

Existing Environment

- Windows Server 2019 IIS behind a load balancer and within an Auto Scaling Group
- AWS RDS SQL Server 2019 database (shared with Colectica)
- S3 for Static Files, ALB Logs and Backups
- 2 IP restricted websites

Architecture Diagram

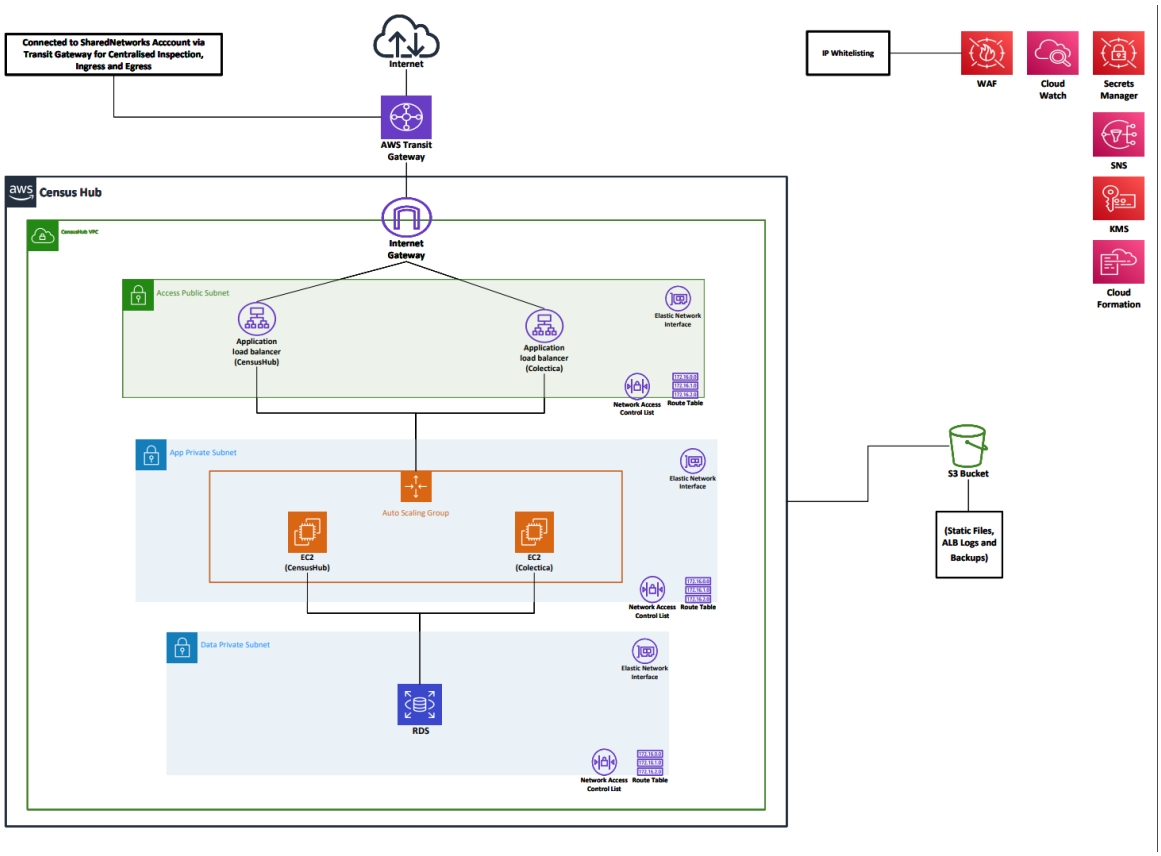

Figure 5 Census hub Architecture Diagram

4.2.6 Virtual Data Rooms (VDR)

Background

The Virtual Data Rooms (VDR) application allows researchers (e.g. Universities) and external Civil and Public Service (CPS) organisations to apply to the CSO for access to data. Research Projects allow a group of researchers to apply for access to data. Upon approval of a project the researchers will each get access to a Project VDI in the RES (Research and engineering studio) environment, the data is transferred to their secure area, and it allows them to access the data. Researchers can then request outputs from their project through the system, which, if approved, are emailed to the researchers.

The application includes a Front-End application (S3 static bucket) fronted by a CloudFront distribution and a C# backend app running on Windows IIS. Authentication is managed by SSO via Entra.

AWS Research and Engineering Studio (RES) is used within the VDR application to facilitate the restricted data access for external researchers to support research and analysis in a secure environment. External researchers are required to be able to view data files within projects, perform analysis and write back outputs.

Key Stakeholders

Internal Stakeholders:

- Statistical Business Areas – responsible for dataset creation and maintenance for researchers to access
- CSO VDR Teams – managing application and governance
- Cloud & Cybersecurity Division – responsible for looking after the relative competencies.
- CSO Senior Leadership – responsible for approving datasets for use

External Stakeholders:

- Civil and Public Service organisations conducting statistical analysis
- Approved external researchers

Existing Configuration

- Front-end static web application hosted on AWS S3 and distributed via CloudFront
- Backend C# (.NET) application hosted on Windows IIS
- Memcached installed locally
- Per-project isolated VDI environments
- Pseudonymisation applied prior to dataset release
- Multi-factor authentication with SSO-based access
- No direct internet access from VDR environment
- Only outputs approved by CSO and meeting confidentiality requirements can be shared outside the VDR.

Existing Environment

- Uses JavaScript, CSS, HTML5
- Windows Server & Linux server tier
- Data residency restricted to Ireland via AWS WAF geoblocking
- Server Application developed in .Net 8/10 Also uses JS, CSS, and HTML5.
- AWS RDS SQL Server 2022 database
- AWS SES for email functions
- Data access is managed in accordance with regional policy requirements.
- Tools inside VDI's: R, Python, Office Libre
- FSx for development
- FSx for windows server data access
- S3 for linux server data access

Existing Configuration

VDR has three environments:

- Production
- UAT
- Development

Background Services

None

Interfaces

None

Server Details

- VDR Admin
    - Windows
- VDR
    - Linux VDIs
    - Windows VDIs

Architecture Diagram

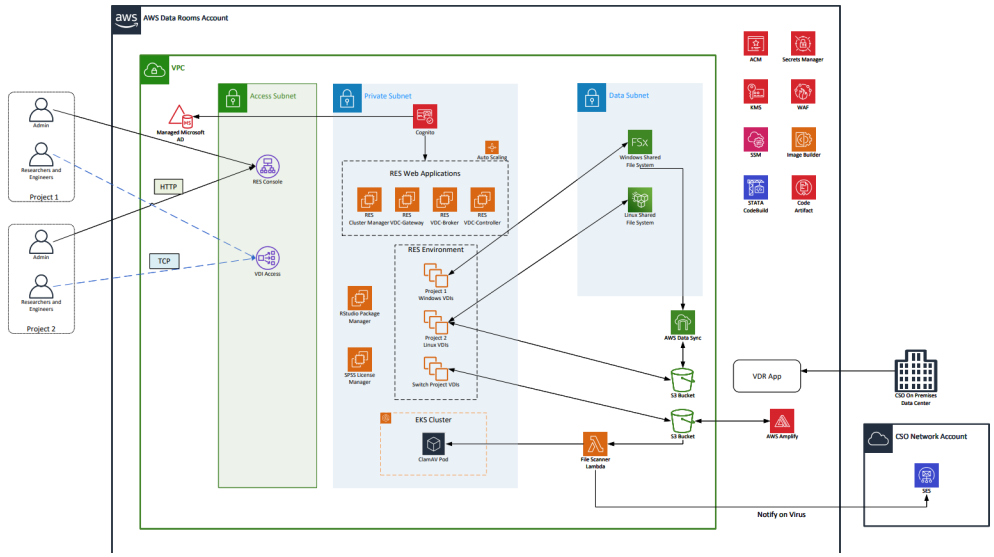

Figure 6 Research and Engineering Studio Architecture Diagram

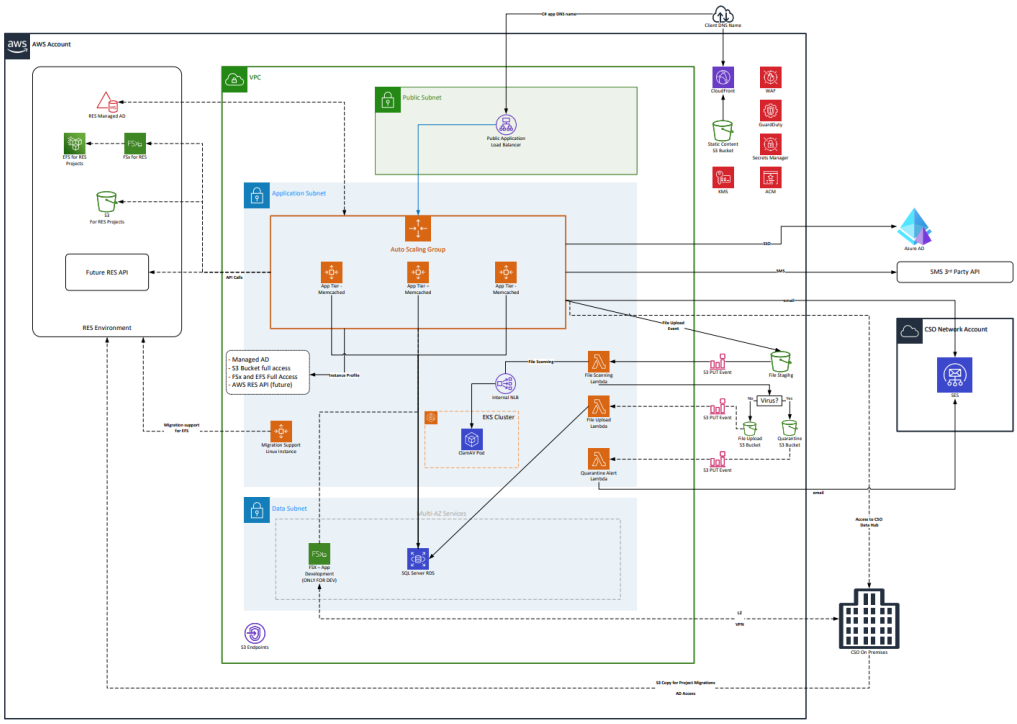

Figure 7 VDR Admin Architecture Diagram

4.2.7 Colectica

Background
Colectica is a standards-based metadata management platform used by the CSO to document, manage, and publish statistical metadata in accordance with the Data Documentation Initiative (DDI) standard, including DDI Codebook and DDI Lifecycle.

The platform supports the structured documentation of surveys, statistical classifications, concepts, variables, and associated metadata. It promotes harmonisation, comparability, and consistency of statistical outputs across the Irish Public and Civil Service.

The metadata portal (metadataddi.cso.ie) provides access to structured metadata relating to CSO surveys and classifications.

Key Stakeholders
Internal Stakeholders:
- Statistical Business Areas – responsible for creating and maintaining survey metadata
- CSO Colectica Team – responsible for metadata standardisation
- Infrastructure Division – responsible for looking after the relative competencies.
- Cloud & Cybersecurity Division – responsible for looking after the relative competencies.
- Statistical Business Areas – responsible for dataset creation and maintenance for researchers to access

External Stakeholders:
- Government Departments responsible for publishing statistics
- National and international statistical bodies
- General public: consumes the data.
- Open-source statistical community

Existing Configuration
- Single page application using a static website
- Implemented by CSO in Ireland (at metadataddi.cso.ie)
- Metadata storage repository aligned with open (DDI) standards
- Metadata portal for browsing and publishing documentation.
- Tools for questionnaire design, metadata import/export, repository synchronization.
- It is a central question bank to enable the reuse of standard questions.
- It enables us to view all metadata items including for example surveys, questionnaires and related documentation.
- Provides a platform to review the data across the **Generic Statistical Business Process Model** (GSBPM).
- Provides functionality to standardise content and improve metadata across all surveys.

- Enables the production of survey forms, quality reports and codebooks and other survey documentation.
- Enables version control and traceability of item changes over time
- Metadata items can be downloaded in PDF, XML and DDI.

Existing Environment

- Web portal component for metadata publication.
- IIS Windows Colectica software
- .NET (8/10) server application
- JavaScript, CSS, HTML5
- Windows Server 2019
- AWS RDS SQL Server 2019 database (shared with CensusHub)

Existing Configuration

Colectica has one environment:

- Production

Background Services

None

Interfaces

None

Server Details

- Windows 2019 Datacentre 64bit
- 2 vCPU
- 8GB RAM
- 50GB EBS storage

URLs:

- metadataddi.cso.ie
- metadata.cso.ie
- datastandards.cso.ie

Architecture Diagram

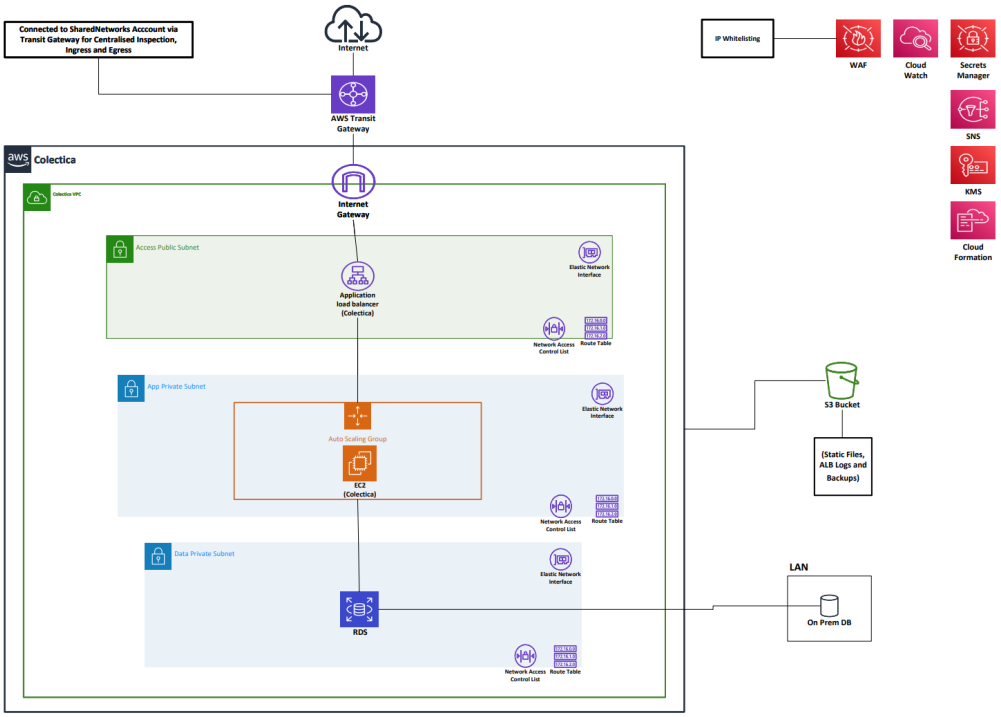

Figure 8 Colectica Architecture Diagram

4.3 Infrastructure-as-Code and Automation Artefacts

IaC Tooling

- AWS CloudFormation is the primary IaC tool in use for provisioning cloud infrastructure
- Assisted by AWS Lambda and AWS EventBridge Scheduler to automate our run time-based scripts e.g. turning off EC2 instances in the Dev Environment during weekends, after work hours and bank holidays.

Automation and Automation Artefacts

- AWS CloudFormation templates are stored in S3 and managed as the primary IaC artefacts
- AWS CloudFormation Stacks and StackSets are used for cross-account resource provisioning. AWS CloudFormation StackSets are managed within our AWS root account.
- AWS Control Tower is in use for landing zone governance and account provisioning

Containerization

- Containerisation (Docker, AWS ECS, AWS EKS) - ONLY in use to run a ClamAV pod in some projects, which is an instance of the ClamAV open-source antivirus engine, used for file scanning and virus detection

4.4 Monitoring, Observability and Alerting

The current monitoring, observability and alerting model operates across both platform and workload layers, combining AWS-native services (e.g. CloudWatch, CloudTrail) with a centralised CSO-owned observability capability using Datadog (including integrated synthetic monitoring via Pingdom). The CSO retains ownership of the observability platform, including configuration, dashboards, and alert definitions, while the MSP is expected to operationally consume and act on alerts generated from this layer.

Alerts will primarily relate to infrastructure health (compute, storage, networking), application performance, availability (including synthetic checks), security signals, and cost anomalies where relevant to operational stability. These alerts are routed through defined channels (e.g. ticketing systems and on-call mechanisms), with the MSP responsible for first-line triage, incident response, and escalation in line with agreed SLAs.

Monitoring coverage spans both underlying cloud platform components and deployed workloads. The MSP shall be responsible for effective operational monitoring and incident detection across the in-scope environment. While the CSO retains ownership of observability tooling and alert configuration, the MSP is expected to identify and escalate any gaps in monitoring coverage, alerting effectiveness, or detection capability that may impact service reliability.

The MSP shall not rely solely on predefined alerts and is expected to apply operational expertise, trend analysis, and anomaly detection techniques, where appropriate, to identify emerging issues that may not yet be captured through existing alerting mechanisms.

Escalation paths will include hand-off to CSO teams for deeper architectural or application-level intervention where required. The MSP shall retain ownership of incident coordination and resolution activities, including engagement with CSO teams and third parties, until service restoration is achieved.

Current limitations include alert noise due to inconsistent thresholding, duplication across tools, and some gaps in end-to-end visibility for certain legacy or partially onboarded services. The MSP shall actively contribute to the continuous improvement of alert quality, including tuning, noise reduction, and enhancement of monitoring coverage, and shall provide regular recommendations to the CSO to improve overall observability effectiveness within the defined CSO-led framework.

4.5 Current Service Desk Ticket Volumes

The following table provides an indicative summary of tickets raised by the CSO with the current managed service provider’s service desk for the period September 2025 to April 2026. This information is provided for background and tender sizing purposes only. It is not a commitment, guarantee or forecast of future ticket volumes, ticket mix or support demand under the Contract.

Table 1: Tickets raised by the CSO with the current MSP's service desk for September 2025 to April 2026

Total Tickets Raised	P1	P2	P3	P4	Lowest
141	8	6	119	7	1

Tenderers should take this historic ticket profile into account when describing their proposed service desk, incident management, escalation, reporting and resourcing model, while recognising that actual future volumes may vary.

Please note: The priority labels in Table 1 reflect historic classifications used in the incumbent service desk tool and do not amend or extend the SLA severity model to be agreed under this Contract.

4.6 Retained CSO Responsibilities and Interfaces

The live operating model is based on a retained strategic control with a collaborative delivery partnership, where the CSO maintains overall accountability for governance, financial management, and service direction, while the MSP is responsible for day-to-day operations and contributes to continuous service improvement.

The CSO retains ownership of AWS commercial management, including account structure, billing, and vendor engagement with AWS. FinOps and cloud financial governance are led by the CSO, covering budgeting, forecasting, and cost control. This operates as a joint function, with the MSP supporting the CSO by providing optimisation recommendations, usage insights, and identifying cost anomalies and efficiency opportunities, as well as supporting the implementation of cost optimisation measures.

The observability platform (Datadog and integrated tooling) is CSO-owned, including standards, configuration, and roadmap. The MSP consumes alerts and telemetry for operational response, and works in partnership with the CSO to refine alerting, reduce noise, and improve monitoring coverage over time.

Governance of architecture, security, and change management follows a shared model, where the CSO defines standards, policies, and approval frameworks, and the MSP contributes technical input, supports design decisions, and executes approved changes. Operational decisions may be delegated to the MSP within agreed guardrails; however, all changes impacting architecture, security posture, or cost must follow CSO-defined approval processes.

The MSP shall operate within this model while maintaining accountability for end-to-end service operation and incident resolution, including coordination across CSO teams and third-party providers where required.

The model is underpinned by structured engagement, including service reviews, operational forums, and defined escalation pathways, ensuring clear accountability while enabling a collaborative, outcome-focused partnership between the CSO and the MSP

5 Categorisation of Core Requirements

The CSO has categorised the requirements set out in this Appendix using a priority classification that applies to each individual requirement. The priority levels are defined as follows (in descending order of importance):

- **Mandatory (Must):** The requirement is compulsory. Tenderers must confirm full compliance. Failure to meet a Mandatory requirement may result in the Tender being deemed non-compliant.
- **Desired (Should):** The requirement is important but not mandatory. Tenderers are expected to meet the requirement where possible. Where full compliance is not offered, Tenderers shall provide an explanation and may propose an alternative approach or workaround for evaluation by the CSO.
- **Could:** The requirement is optional and not essential to core service delivery. While beneficial, failure to meet a Could requirement will not render a Tender non-compliant but may be considered during qualitative evaluation.

Only requirements explicitly identified in the tables as Mandatory, Desired or Could form part of the evaluation and contractual compliance framework.

6 Scope of Managed Services

The scope of the Managed Services under this Contract comprises the ongoing operational management, support and optimisation of the CSO's existing cloud environment from the existing landing zone and core platform services through to the in-scope workloads and applications. The MSP shall deliver these services in accordance with CSO-defined governance, security and approval controls to ensure service stability, regulatory compliance and cost efficiency.

6.1 Cloud Platform Operations

Requirement	Priority
Core Operational Management	
The MSP shall provide day-to-day operational management of the CSO's existing AWS infrastructure and platform services.	Mandatory
The MSP shall provide monitoring, alerting and event management across all in-scope workloads and cloud services.	Mandatory
The MSP shall provide proactive fault identification, investigation and remediation to minimise service disruption.	Mandatory
The MSP shall perform routine maintenance activities and ensure ongoing platform hygiene in accordance with agreed operational standards.	Mandatory
The MSP shall operate and maintain automation and infrastructure-as-code artefacts where implemented within the existing cloud environment.	Mandatory
The MSP shall provide operational support and management for the in-scope workloads and applications operating within the existing cloud environment.	Mandatory
Operation and Management of Existing Landing Zone(s)	
The MSP shall operate, manage and maintain the CSO's existing Landing Zone(s), ensuring continued alignment with agreed operational principles, technical standards and security requirements.	Mandatory
The MSP shall ensure that the existing Landing Zone(s) continue to provide, at a minimum: appropriate network configuration, connectivity and security controls; standardised management, monitoring and reporting capabilities; resource allocation and configuration management mechanisms; and access control aligned to the principle of least privilege.	Mandatory
The MSP shall maintain up-to-date operational documentation relating to the Landing Zone(s).	Mandatory
The MSP shall support the ongoing optimisation and controlled evolution of the existing Landing Zone(s), subject to CSO approval and governance processes.	Desired
Workload Inventory and Governance Controls	
The MSP shall maintain and manage an up-to-date inventory of in-scope cloud workloads, services and configurations to support effective operational management, reporting and governance.	Mandatory
Operational Risk Management	
The MSP shall support the CSO in identifying, managing and mitigating operational risks associated with the ongoing operation, scaling or decommissioning of workloads within the existing cloud environment.	Mandatory

6.2 Resource Location, Data Access and Restricted Access Roles

Requirement	Priority
The MSP shall ensure that all Restricted Access Roles are performed only by personnel located Onshore or Nearshore, as defined in Appendix 1, Part D of the RFT.	Mandatory
Offshore Personnel shall not perform, support, backfill, supervise or provide escalation support for any Restricted Access Role and shall not have logical, remote, administrative, privileged, monitoring, service desk, security, incident-response or support access to CSO Data, CSO Confidential Information, the Managed Environment, service desk records, logs, telemetry, observability outputs, IAM functions, credentials or secrets.	Mandatory
Any proposed Offshore use shall be limited to ancillary corporate or administrative functions that do not involve access to CSO Data, CSO Confidential Information, the Managed Environment, tickets, logs, telemetry, repositories, documentation, credentials or secrets, and shall require prior CSO approval.	Mandatory
Where the MSP proposes to use personnel located in the United Kingdom, including Northern Ireland, for any Restricted Access Role, the MSP shall maintain a documented contingency plan to ensure that such role can be transitioned to personnel located Onshore or within the EEA if the United Kingdom ceases to qualify as Nearshore under Appendix 1, Part D of the RFT.	Mandatory
The contingency plan outlined in the previous requirement shall address, as a minimum, replacement resourcing, service continuity, SLA continuity, access removal, privileged access controls, session management, audit logging, subcontractor or affiliate arrangements, knowledge transfer, security controls, data protection compliance and any operational impact on the managed service.	Mandatory
If the United Kingdom ceases to qualify as Nearshore in accordance with Appendix 1, Part D of the RFT, the MSP shall implement the contingency plan within the timeframe specified by the CSO and shall ensure that no Restricted Access Role is performed by UK-based personnel from the date specified by the CSO.	Mandatory
No additional charges, uplifts or claims shall apply solely as a result of the MSP being required to implement its contingency plan or otherwise comply with the CSO's Onshore, Nearshore and Offshore requirements following any change in the status of the United Kingdom under Appendix 1, Part D of the RFT.	Mandatory

6.3 Service Desk and Operational Support

Requirement	Priority
Service Desk Model and Coverage	
The MSP shall operate a fully resourced service desk aligned to recognised best practice (e.g. ITIL) to support cloud-related incidents and service requests.	Mandatory

The MSP shall provide a 24x7 support solution and a staffed telephone service desk during office hours (Monday–Friday, 8:00am–7:00pm Irish time, excluding public holidays).	Mandatory
The MSP shall provide a 24/7/365 staffed Network Operations Centre (NOC) and Security Operations Centre (SOC).	Mandatory
The SOC service shall include SIEM-based security event ingestion, monitoring and correlation, as well as alert triage, investigation, and escalation in respect of the managed service, including relevant alerts arising from CSO-operated cloud observability and SIEM tooling, in accordance with agreed security processes and service boundaries.	Mandatory
The MSP shall provide Level 1 (L1), Level 2 (L2) and Level 3 (L3) support capabilities.	Mandatory
The MSP shall clearly identify the location from which each service desk, NOC, SOC and L1/L2/L3 support function will be delivered, including whether such functions will be delivered onshore, nearshore and/or offshore.	Mandatory
Where any service desk, NOC, SOC or L1/L2/L3 support function is delivered from outside Ireland or outside the EEA, the MSP shall describe the applicable governance, security, access control, data protection and escalation arrangements.	Mandatory
The MSP shall ensure service desk coverage for both production and non-production environments within the existing cloud estate.	Mandatory
The MSP shall be capable of providing increased service capacity and enhanced operational support during agreed peak operational periods, as notified by the CSO.	Mandatory
Service Desk Tooling and Access	
The MSP shall provide the CSO with access to its service desk tool to support the logging, tracking, management and reporting of incidents and service requests.	Mandatory
The service desk tool shall maintain a complete audit trail including, as a minimum: unique identifier, issue description, classification, associated assets, activity history, resolution details and closure status.	Mandatory
The MSP shall integrate its incident and operational response processes with relevant alerts arising from CSO-operated cloud observability tooling, where such alerts relate to the managed service.	Mandatory
Incident and Request Handling Processes	
The MSP shall operate robust processes for incident and request logging, classification, prioritisation, escalation, notification and reporting.	Mandatory
The MSP shall prioritise incidents raised by the CSO or through monitoring systems in accordance with agreed severity definitions. Incident priorities shall not be amended without the explicit agreement of the CSO.	Mandatory
The MSP shall coordinate with relevant third-party suppliers where required to support incident resolution, in accordance with agreed governance arrangements.	Mandatory
Support Response and Resolution Targets	
The MSP shall meet agreed response and resolution targets for incidents in accordance with the Service Level Agreement (SLA).	Mandatory
Severity P1 (Critical) incidents shall have an initial response target of 20 minutes and a resolution time objective of 4 hours from initial notification, alert or ticket logging.	Mandatory
Severity P2 (Major) incidents shall have an initial response target of 20 minutes and a resolution time objective of 8 hours from initial notification, alert or ticket logging.	Mandatory
Severity P3 (Minor) incidents shall have an initial response target of 4 hours and a resolution time objective of 48 hours from initial notification, alert or ticket logging.	Desired
Where the CSO requires increased service levels or enhanced support for defined operational periods, the applicable service arrangements and service levels shall be agreed in advance.	Mandatory

Escalation and Communication Controls	
The MSP shall provide a clearly defined escalation path including named contacts, email addresses and telephone numbers for operational and executive escalation.	Mandatory
The MSP shall provide defined 24x7 support and escalation contact details.	Mandatory
The MSP shall provide advance notification of scheduled upgrades, fixes or maintenance activities and allow the CSO the opportunity to raise concerns prior to implementation.	Mandatory

7 Service Management Framework

The MSP shall operate a formal service management framework aligned to recognised best practice (e.g. ITIL). The framework shall be documented, measurable and subject to continuous improvement.

7.1 Service Management Governance Model

Requirement	Priority
The MSP shall operate a documented service management framework aligned to recognised industry best practice (e.g. ITIL).	Mandatory
The framework shall define roles, responsibilities and governance arrangements between the MSP and the CSO, including a clearly documented RACI model where applicable.	Mandatory
The MSP shall ensure that all service management processes operate in accordance with CSO-defined policies, standards and approval controls.	Mandatory
The framework shall reflect the agreed operational interfaces between the MSP and the CSO, including the handling and escalation of relevant alerts arising from CSO-operated cloud observability tooling where such alerts relate to the managed service.	Mandatory
The service management framework shall be measurable and subject to continuous improvement, supported by defined KPIs and reporting mechanisms.	Mandatory

7.2 Core Service Management Processes

Requirement	Priority
The service management framework shall include documented processes for Incident Management.	Mandatory
The service management framework shall include documented processes for Problem Management.	Mandatory
The service management framework shall include documented processes for Change Management.	Mandatory
The service management framework shall include documented processes for Release Management.	Mandatory
The service management framework shall include documented processes for Configuration Management.	Mandatory
The service management framework shall include documented processes for the handling, triage, escalation and resolution of relevant alerts arising from CSO-operated cloud observability tooling, where such alerts relate to the managed service.	Mandatory

The service management framework shall include documented processes for the planning and management of enhanced service arrangements during agreed peak operational periods.	Mandatory
The service management framework shall include documented processes for the onboarding and operational enablement of new workloads introduced within the existing cloud environment, including governance, approval, handover and service readiness requirements.	Mandatory

7.3 Configuration and Asset Control

Requirement	Priority
The MSP shall maintain accurate configuration and asset records for in-scope cloud services and workloads to support governance, reporting and audit requirements.	Mandatory
Configuration data shall be maintained in a controlled and auditable manner and kept current throughout the contract term.	Mandatory

7.4 Continuous Service Improvement

Requirement	Priority
The MSP shall support periodic service reviews and continuous improvement initiatives to enhance performance, resilience, security and service effectiveness within the existing cloud environment.	Mandatory
The MSP shall identify and recommend operational improvements based on service performance data, trend analysis and industry best practice.	Desired
The MSP shall identify and recommend service improvements arising from recurring incidents, operational trends, lessons learned and relevant alerts generated through CSO-operated cloud observability tooling, where such alerts relate to the managed service.	Desired

7.5 Sustainable Service Delivery and Operational Efficiency

Requirement	Priority
The MSP shall support sustainable service delivery through the efficient operation, management and continuous improvement of the managed service.	Desired
The MSP shall identify and recommend opportunities to improve operational efficiency, including efficient resource utilisation, reduction of unnecessary	Desired

consumption, and avoidance of wasteful or duplicative operational activity within the managed service.	
The MSP shall, where relevant to the managed service, identify opportunities to minimise energy consumption and environmental impact through appropriate operational practices, optimisation recommendations and use of efficient cloud service configurations, subject to CSO approval.	Desired
The MSP shall report, where appropriate, on sustainability-related service improvements and operational efficiency measures through the service review and continuous improvement process.	Desired

8 Incident, Problem, and Major Incident Management

The MSP shall operate structured and documented processes for incident, problem and major incident management to ensure timely restoration of service, effective communication and continuous improvement, including in relation to relevant alerts arising from CSO-operated cloud observability tooling where such alerts relate to the managed service.

8.1 Incident Classification and Prioritisation

Requirement	Priority
The MSP shall operate a documented incident classification and prioritisation model aligned to agreed severity definitions.	Mandatory
Severity definitions shall be defined and approved by the CSO and applied by the MSP in accordance with agreed service management processes.	Mandatory
Incident classification and prioritisation shall directly determine applicable service levels, including response and resolution targets.	Mandatory
Incident categorisation and prioritisation shall be consistently applied and auditable, including where incidents arise from monitoring systems or relevant alerts generated through CSO-operated cloud observability tooling.	Mandatory
Incident classification and prioritisation shall be applied consistently across all incident sources, including user-reported incidents, automated alerts, and monitoring systems.	Mandatory
Incident priorities shall not be amended without the explicit agreement of the CSO.	Mandatory
Any proposed reclassification of an incident shall require CSO approval and must be documented and auditable.	Mandatory
Severity P1 (Critical) incidents shall be treated as Major Incidents and managed in accordance with the defined Major Incident Management process.	Mandatory

8.2 Incident Response and Escalation

Requirement	Priority
The MSP shall maintain clearly defined response and escalation procedures for all incident categories, including incidents or event escalations arising from relevant alerts generated through CSO-operated cloud observability tooling.	Mandatory
The MSP shall ensure that escalation procedures include technical, managerial and executive escalation paths as appropriate.	Mandatory

The MSP shall ensure that communication with the CSO during incidents is timely, structured and proportionate to the severity of the issue, including during agreed peak operational periods where enhanced service arrangements apply.	Mandatory
The MSP shall retain responsibility for incident management and service restoration, including coordination with CSO teams, AWS, and third-party suppliers, until full service restoration is achieved.	Mandatory
The MSP shall ensure that incidents are logged, tracked, and managed through to resolution in accordance with agreed service levels and governance processes.	Mandatory
The MSP shall ensure that incident management processes are applied consistently across all incident sources, including user-reported incidents, automated alerts, and monitoring systems.	Mandatory
The MSP shall implement a structured Major Incident Management process for Severity P1 (Critical) incidents.	Mandatory
The MSP shall appoint a Major Incident Manager for each P1 incident, responsible for coordinating all activities and communications.	Mandatory

8.3 Major Incident Management

Requirement	Priority
The MSP shall operate a formal Major Incident procedure aligned with the CSO's Incident Response Plan, including where a Major Incident is triggered or escalated through relevant alerts arising from CSO-operated cloud observability tooling.	Mandatory
For each Major Incident (Critical or High), the MSP shall appoint a Major Incident Manager responsible for coordinating recovery activities and stakeholder communications.	Mandatory
The MSP shall ensure command and control arrangements are implemented during Major Incidents to minimise service disruption and business impact.	Mandatory
The MSP shall liaise with relevant third parties and AWS technical support where required to expedite resolution of Major Incidents.	Mandatory
The MSP shall ensure that Major Incident procedures remain effective during agreed peak operational periods where enhanced service arrangements apply.	Mandatory

8.4 Root Cause Analysis and Post-Incident Review

Requirement	Priority

The MSP shall provide formal post-incident reports for Major Incidents, including detailed root cause analysis, impact assessment and corrective actions.	Mandatory
The MSP shall document lessons learned and track corrective actions to closure, including actions arising from incidents or escalations generated through CSO-operated cloud observability tooling where relevant to the managed service.	Mandatory

8.5 Problem Management and Trend Analysis

Requirement	Priority
The MSP shall operate a documented Problem Management process to identify, investigate and eliminate the underlying causes of recurring incidents.	Mandatory
The MSP shall conduct periodic trend analysis of incident data to identify systemic risks and improvement opportunities, including trends arising from relevant alerts generated through CSO-operated cloud observability tooling.	Mandatory
The MSP shall proactively recommend preventive measures to reduce incident recurrence and improve service stability.	Desired

9 Change, Release, and Patch Management

The MSP shall operate structured and controlled change, release and patch management processes to ensure service stability, risk mitigation and compliance with CSO governance requirements, including in relation to changes arising from relevant alerts generated through CSO-operated cloud observability tooling where such alerts relate to the managed service.

9.1 Change Management Governance

Requirement	Priority
The MSP shall manage standard, normal and emergency changes in accordance with a documented Change Management process.	Mandatory
The MSP shall operate clearly defined approval boundaries between the MSP and the CSO for all change categories, including changes relating to existing services and any new or amended workloads brought into the managed service.	Mandatory
No change impacting service availability, security or cost shall be implemented without prior CSO approval, except where emergency change procedures apply.	Mandatory
The MSP shall maintain a Forward Schedule of Change (FSC) accessible to the CSO.	Mandatory
The Change Management process shall include the assessment, classification and escalation of changes arising from relevant alerts generated through CSO-operated cloud observability tooling, where such alerts relate to the managed service.	Mandatory
The MSP shall ensure that planned changes are coordinated appropriately during agreed peak operational periods and other business-critical windows notified by the CSO.	Mandatory

9.2 Release Management

Requirement	Priority
The MSP shall coordinate release activities to minimise service disruption and operational risk.	Mandatory
Release activities shall include documented testing, validation and rollback planning prior to implementation, including where releases relate to new or amended workloads entering or changing within the managed service.	Mandatory
The MSP shall ensure that release documentation is maintained and available for audit and governance purposes.	Mandatory
The MSP shall ensure that release planning takes account of relevant alerts, dependencies and operational risks identified through CSO-operated cloud observability tooling, where such alerts relate to the managed service.	Mandatory
The MSP shall ensure that release activities are planned and controlled appropriately during agreed peak operational periods and other business-critical windows notified by the CSO.	Mandatory

9.3 Patch Management

Requirement	Priority
The MSP shall operate a controlled patch management process across the CSO's existing public cloud environment.	Mandatory

The MSP shall actively monitor vendor notifications, security advisories and patch releases relevant to in-scope systems and services.	Mandatory
The MSP shall assess patch severity and prioritise deployment based on recognised vulnerability classification frameworks and risk assessment.	Mandatory
The MSP shall test patches in appropriate non-production environments prior to deployment.	Mandatory
The MSP shall maintain documented rollback procedures to restore services to a stable state where patching introduces issues.	Mandatory
The MSP shall manage patch deployment within agreed maintenance windows and change governance processes.	Mandatory
The MSP shall track and report patch compliance and outstanding vulnerabilities to the CSO.	Mandatory
The MSP shall take account of relevant alerts and operational dependencies identified through CSO-operated cloud observability tooling when assessing patch urgency, deployment planning and escalation, where such alerts relate to the managed service.	Mandatory
The MSP shall ensure that patch deployment planning reflects agreed business-critical windows and peak operational periods notified by the CSO.	Mandatory

9.4 Vulnerability Integration

Requirement	Priority
The MSP shall ensure that vulnerability management outputs are integrated into the patch and change management process to ensure timely remediation of identified risks, including where relevant vulnerabilities are identified or escalated through CSO-operated cloud observability tooling and related managed service processes.	Mandatory
High-risk vulnerabilities shall be prioritised in consultation with the CSO Cloud Team.	Mandatory

10 Availability, Capacity, and Resilience Management

The MSP shall ensure the continuous availability, performance, capacity sufficiency and resilience of the CSO's existing cloud environment from the existing Landing Zone(s) and core platform services through to the in-scope workloads and application in support of business-critical services, including peak operational events such as Census and survey cycles.

10.1 Availability and Performance Monitoring

Requirement	Priority
The MSP shall continuously monitor availability and performance across all in-scope cloud services and workloads, including in-scope applications and relevant service dependencies.	Mandatory
Monitoring shall include proactive alerting where defined thresholds are breached or service degradation is detected, including relevant alerts arising from CSO-operated cloud observability tooling where such alerts relate to the managed service.	Mandatory
The MSP shall analyse performance metrics to identify bottlenecks and recommend optimisation measures, including in advance of and during agreed peak operational periods.	Mandatory
The MSP shall implement approved optimisation measures to maintain agreed service levels, including any agreed enhanced service arrangements for defined peak operational periods.	Mandatory

10.2 Capacity Management and Forecasting

Requirement	Priority
The MSP shall perform regular capacity planning using utilisation data, performance metrics and forecast demand, including demand associated with in-scope applications and relevant service dependencies.	Mandatory
The MSP shall provide capacity and utilisation reporting, including trends and forward-looking forecasts.	Mandatory
The MSP shall manage and operate scaling and elasticity mechanisms within the existing cloud environment.	Mandatory
Scaling policies shall be aligned to agreed operational standards and CSO approvals.	Mandatory
The MSP shall ensure readiness for peak operational events, including Census and major survey cycles , and shall support any agreed enhanced service arrangements applicable during such periods.	Mandatory
Capacity planning and forecasting shall take account of relevant alerts, utilisation trends and operational indicators arising from CSO-operated cloud observability tooling, where such alerts relate to the managed service.	Mandatory

10.3 Business Continuity and Disaster Recovery

Requirement	Priority
The MSP shall maintain, operate and periodically review a Disaster Recovery Plan (DRP) aligned with the CSO's Business Continuity framework.	Mandatory
The DRP shall define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) in consultation with the CSO.	Mandatory

The MSP shall conduct periodic disaster recovery testing and provide documented test results.	Mandatory
The MSP shall support recovery exercises and continuous improvement of resilience arrangements.	Mandatory
The DRP and related recovery arrangements shall take account of in-scope applications, service dependencies and agreed business-critical periods notified by the CSO.	Mandatory
The MSP shall take account of relevant alerts, risk indicators and operational dependencies identified through CSO-operated cloud observability tooling when supporting continuity and disaster recovery preparedness, where such alerts relate to the managed service.	Mandatory

10.4 Backup, Replication and Failover

Requirement	Priority
The MSP shall manage and monitor backup processes to ensure availability and integrity of critical data and the continued recoverability of in-scope workloads and applications.	Mandatory
Backup operations shall include verification of backup success and periodic restoration testing, including validation during agreed business-critical periods where required by the CSO.	Mandatory
The MSP shall manage replication and failover mechanisms for critical systems and services, including relevant in-scope applications and service dependencies.	Mandatory
Failover procedures shall be periodically tested to validate operational readiness, taking account of agreed peak operational periods and business-critical windows notified by the CSO.	Mandatory
The MSP shall take account of relevant alerts and operational indicators arising from CSO-operated cloud observability tooling when managing backup, replication and failover activities, where such alerts relate to the managed service.	Mandatory

11 Workload Support, Optimisation, and Lifecycle Management

The MSP shall provide operational support, controlled onboarding, optimisation and lifecycle management of CSO workloads deployed within the existing cloud environment, including the associated in-scope applications and relevant service dependencies. The scope relates to the ongoing management of workloads and does not include the design or build of a new cloud platform.

11.1 Operational Support for In-Scope Workloads

Requirement	Priority
The MSP shall provide ongoing operational support and maintenance for all in-scope CSO workloads hosted within the existing cloud environment, including the associated in-scope applications.	Mandatory
Operational support shall include performance monitoring, configuration management and incident coordination in accordance with agreed service levels, including the handling of relevant alerts arising from CSO-operated cloud observability tooling where such alerts relate to the managed service. Operational support does not include software development or material code change unless expressly agreed through a Statement of Work or formal change control process.	Mandatory
The MSP shall ensure workload stability, availability and security are maintained in alignment with CSO standards and agreed service requirements.	Mandatory

11.2 Workload Onboarding and Enablement

Requirement	Priority
The MSP shall operate a standardised workload onboarding process aligned to agreed operational standards, governance controls and security requirements, including service readiness and operational handover into the managed service.	Mandatory
The onboarding process shall include scope definition, prerequisites, dependencies, configuration validation, testing and formal approval prior to go-live together with confirmation of the applicable service requirements for the onboarded workload.	Mandatory
Where onboarding requires discrete project-based activities, such work shall be governed by an agreed Statement of Work (SoW) approved by the CSO prior to commencement. The SoW shall, as a minimum, define the scope of work, project scope, dependencies, assumptions, risks, desired service level, ongoing service requirements for the new or amended workload, and any additional requirements necessary to support transition into the managed service.	Mandatory

The MSP shall ensure that onboarded workloads comply with agreed identity, network, security and data protection standards.	Mandatory
The MSP shall maintain appropriate documentation for all onboarded workloads and provide knowledge transfer to the CSO Cloud Team.	Mandatory

11.3 Interoperability and Integration

Requirement	Priority
The MSP shall ensure interoperability of new or amended workloads with existing CSO technologies and platforms.	Mandatory
Required integrations and validations shall be implemented and tested to support stable and secure operations, prior to operational handover into the managed service.	Mandatory

11.4 Optimisation and Technical Debt Management

Requirement	Priority
The MSP shall support ongoing optimisation of workloads, including performance, resilience and operational efficiency initiatives, subject to CSO approval.	Mandatory
The MSP shall identify and recommend opportunities to reduce technical debt within the existing workload estate.	Desired
The MSP shall advise on appropriate use of cloud-native services and automation approaches (e.g. infrastructure-as-code, containers, serverless services) where beneficial and subject to CSO approval.	Desired
The MSP shall not assume responsibility for FinOps or cloud financial governance, which shall remain solely with the CSO	Mandatory

11.5 Workload Decommissioning and Retirement

Requirement	Priority
The MSP shall support the controlled decommissioning and retirement of workloads in accordance with agreed governance and data retention requirements including the decommissioning of amended or replaced workloads where applicable.	Mandatory
Decommissioning activities shall include documentation updates, secure data handling and removal of associated resources together with the completion of any required operational handover and service record updates.	Mandatory

11.6 Future Workloads within the Existing Cloud Environment

Requirement	Priority
The MSP shall support the onboarding and operational enablement of new workloads introduced within the CSO's existing cloud environment during the contract term.	Mandatory
Any new workloads shall be onboarded in accordance with agreed operational, security, governance and change management standards.	Mandatory
The introduction of new workloads shall not constitute a redesign or rebuild of the underlying cloud platform.	Mandatory
Where new workload onboarding requires discrete project-based activities outside routine operational scope, such activities shall be governed by an agreed Statement of Work (SoW) approved by the CSO prior to commencement.	Mandatory
The SoW for any new or amended workload shall, as a minimum, define the scope of work, project scope, dependencies, assumptions, risks, desired service level, ongoing service requirements and any additional requirements necessary to support transition into the managed service. The SoW shall also define the recurring support and maintenance requirements applicable following service commencement of the new or amended workload.	Mandatory
Any project-based activities relating to new or amended workloads shall be treated separately from routine managed service activities and shall be governed in accordance with the applicable pricing model set out elsewhere in the RFT.	Mandatory

12 Cybersecurity Operations and Assurance

The MSP shall provide operational cybersecurity services to support the secure operation of the CSO's existing cloud environment and the associated in-scope workloads and applications. Strategic security policy, governance and risk ownership remain the responsibility of the CSO.

12.1 Security Monitoring and Threat Detection

Requirement	Priority
The MSP shall provide continuous security monitoring across all in-scope cloud services and workloads, including associated in-scope applications where relevant to the managed service.	Mandatory
Security monitoring shall include SIEM-based event ingestion, detection, correlation, alerting and investigation in accordance with agreed procedures, including the handling of relevant security alerts arising from CSO-operated cloud observability and SIEM tooling where such alerts relate to the managed service.	Mandatory
The MSP shall ensure that relevant security telemetry and log data are collected, retained and made available for analysis and audit purposes.	Mandatory
The MSP shall escalate security incidents in accordance with agreed incident severity definitions and CSO procedures.	Mandatory
The MSP shall operate security monitoring, alert triage, investigation and escalation in accordance with agreed security service boundaries and operational interfaces with the CSO, including, where relevant, security-related alerts arising from CSO-operated cloud observability tooling.	Mandatory
The MSP shall monitor and maintain secure configuration baselines for all in-scope cloud resources in accordance with CSO-approved standards (NIST & Cyfun)	Mandatory
The MSP shall conduct proactive threat-hunting activities within the managed cloud environment on a scheduled basis or where risk indicators warrant. It should have the ability to plug in indicators of compromise as part of threat hunting.	Mandatory

12.2 Identity and Access Management (IAM) Operations

Requirement	Priority
The MSP shall operate IAM processes including role management, access provisioning and de-provisioning in accordance with the principle of least privilege.	Mandatory
The MSP shall support periodic access reviews in coordination with the CSO.	Mandatory
All access changes shall be subject to agreed change and approval controls.	Mandatory

The MSP shall take account of relevant access-related alerts arising from CSO-operated cloud observability tooling, where such alerts relate to the managed service and IAM operations.	Mandatory

12.3 Vulnerability Management

Requirement	Priority
The MSP shall operate a documented vulnerability management process including scanning, identification and risk-based prioritisation of vulnerabilities.	Mandatory
The MSP shall provide reporting on identified vulnerabilities, associated risk ratings and recommended remediation actions.	Mandatory
High-risk vulnerabilities shall be prioritised in consultation with the CSO Cloud Team.	Mandatory
Vulnerability remediation activities shall be integrated with the Patch and Change Management processes defined in Section 6.	Mandatory
The vulnerability management process shall take account of relevant vulnerability-related alerts arising from CSO-operated cloud observability tooling, where such alerts relate to the managed service.	Mandatory
Risk acceptance of decisions shall remain the responsibility of the CSO unless explicitly delegated in writing	Mandatory

12.4 Security Incident Response Support

Requirement	Priority
The MSP shall support security incident response activities in alignment with the CSO's Incident Response Plan including where a security incident is triggered or escalated through relevant security-related alerts arising from CSO-operated cloud observability tooling.	Mandatory
The MSP shall participate in security incident investigations, containment, recovery and post-incident review activities.	Mandatory
The MSP shall support audit and assurance activities relating to security controls within the managed cloud environment.	Mandatory
The MSP shall demonstrate a robust third party risk management (TPRM) process that identifies, assesses, and mitigates risks arising from the engagement of subcontractors, suppliers and other third parties in the delivery of this contract.	Mandatory
The CSO reserves the right to assess the MSPs information security controls through the issuance of security questionnaires, or equivalent assurance mechanisms at any point during the contract term.	Mandatory

The MSP shall actively engage and coordinate with the CSO's existing contracted Security Operations Centre (SOC) during the investigation, containment, and remediation of security incidents affecting the managed cloud environment, in accordance with agreed incident response procedures.	Mandatory

12.5 Optional Penetration Testing Services

Requirement	Priority
Where requested by the CSO, the MSP may provide penetration testing services for explicitly authorised systems or environments, subject to a clearly defined scope and prior CSO approval.	Could
All testing shall follow recognised industry methodologies and applicable legal, regulatory and CSO policy requirements.	Could
The MSP shall ensure strict confidentiality and controlled handling of all findings arising from testing activities.	Could
The MSP shall provide a formal report summarising findings, risk ratings and recommended remediation actions.	Could
Where requested, the MSP shall support remediation planning in coordination with the CSO Cloud Team.	Could
Tenderers shall demonstrate a proven track record in performing penetration testing exercises within cloud environments.	Could

12.6 Backup, Recovery and Key Management

Requirement	Priority
The MSP shall support security controls protecting backup data from unauthorised access or modification.	Mandatory
The MSP shall assist with restoration activities following security incidents, including ransomware events, in coordination with the CSO.	Mandatory
Backup and recovery operations shall be tested periodically where included in scope.	Mandatory
The MSP shall operate key management processes in accordance with CSO's Cryptographic Controls Policy	Mandatory
The MSP shall not access or export cryptographic keys unless explicitly authorised.	Mandatory

13 Data Protection and Compliance

The MSP shall operate in full compliance with applicable data protection legislation, including the General Data Protection Regulation (GDPR), and shall ensure that all managed services are delivered in accordance with CSO regulatory, contractual and statutory obligations.

The CSO retains data ownership and data controller responsibilities. The MSP shall act strictly within authorised operational parameters.

13.1 GDPR and Legal Compliance

Requirement	Priority
The MSP shall operate in compliance with GDPR and all applicable Irish and EU data protection legislation.	Mandatory
The MSP shall process CSO data strictly in accordance with documented instructions and contractual agreements.	Mandatory
The MSP shall not use CSO data for any purpose other than the delivery of contracted services.	Mandatory
Where UK-based personnel, affiliates or subcontractors are proposed in the delivery of the managed service, the MSP shall monitor and promptly notify the CSO of any material legal, regulatory or operational development that may affect the continued treatment of the United Kingdom as Nearshore, including any change affecting the relevant European Commission adequacy decision or the lawful transfer of personal data from the EEA to the United Kingdom.	Mandatory

13.2 Data Handling and Protection Controls

Requirement	Priority
The MSP shall ensure secure handling of data at rest, in transit and in backup.	Mandatory
The MSP shall enforce least-privilege access controls in alignment with IAM processes defined in Section 12.2.	Mandatory
The MSP shall ensure that data access is logged and auditable.	Mandatory
The MSP shall implement appropriate technical and organisational measures to protect against unauthorised access, alteration, disclosure or destruction of data.	Mandatory

13.3 Data Subject Rights and Regulatory Support

Requirement	Priority
The MSP shall support the CSO in responding to regulatory queries and data protection requests, where such requests relate to managed cloud services strictly within authorised operational parameters and in accordance with CSO instructions.	Mandatory
The MSP shall support the CSO in the preparation of Data Protection Impact Assessments (DPIAs) where required.	Mandatory
The MSP shall notify the CSO without undue delay of any suspected or confirmed personal data breach.	Mandatory

13.4 Data Ownership and Sovereignty

Requirement	Priority
The CSO shall retain full ownership of all data, configurations, documentation and artefacts developed in the course of service delivery including the CSO's cloud observability capability and associated outputs.	Mandatory
The MSP shall not assert ownership or intellectual property rights over CSO data or environment configurations or over the CSO's cloud observability capability.	Mandatory
Where any service resources are located outside the EEA, the MSP shall demonstrate how data protection, security and governance requirements are met.	Mandatory
The MSP shall not treat the existence of a European Commission adequacy decision in respect of any third country, other than the United Kingdom where expressly permitted under Appendix 1, Part D of the RFT, as sufficient to classify personnel or service resources in that third country as Nearshore. Any use of non-EEA and non-UK personnel or service resources shall be treated as Offshore and shall be subject to the restrictions set out in this Appendix.	Mandatory

14 License and Subscription Management

The MSP shall provide operational support in relation to software licence and subscription management within the CSO's existing cloud environment where relevant to the operation of the managed service. Commercial ownership and approval authority remain with the CSO**.**

14.1 License Inventory and Management

Requirement	Priority
The MSP shall maintain a comprehensive and up-to-date inventory of software licences and subscriptions used within the CSO's cloud environment where such licences and subscriptions are relevant to the managed service.	Mandatory
The licence inventory shall include licence types, quantities, expiry dates and associated cost information where available.	Mandatory
The licence inventory shall be maintained in a structured and auditable format accessible to the CSO.	Mandatory

14.2 License Procurement and Renewals

Requirement	Priority
Where explicitly authorised by the CSO, the MSP shall support the procurement and renewal of software licences and subscriptions required for the operation of the cloud environment and the managed service.	Mandatory
All licence-related costs shall be agreed in advance with the CSO and clearly documented within billing and reporting arrangements.	Mandatory
The MSP shall notify the CSO in a timely manner of upcoming licence renewals to avoid service disruption.	Mandatory
The MSP shall not enter into commercial commitments on behalf of the CSO without explicit written authorisation.	Mandatory

14.3 License Optimisation and Cost Control

Requirement	Priority
The MSP shall regularly review licence usage and provide recommendations to optimise licence consumption and support the effective operation of the managed service.	Mandatory

Optimisation recommendations may include consolidation, reallocation or decommissioning of unused licences.	Mandatory
The MSP shall provide periodic reporting on licence usage, costs and optimisation opportunities.	Mandatory

14.4 Vendor and Compliance Management

Requirement	Priority
Where responsible for licence management, the MSP shall act as a single operational point of contact for licence-related matters with software vendors, in line with agreed governance arrangements.	Mandatory
The MSP shall monitor licence usage to support compliance with applicable licence terms.	Mandatory
The MSP shall assist the CSO in preparing for and responding to licence audits conducted by vendors or relevant authorities.	Mandatory
The MSP shall support the management of the licence lifecycle, including onboarding, modification, suspension and de-provisioning of licences in line with CSO approvals where relevant to the managed service.	Mandatory

14.5 Bring-Your-Own-Licence (BYOL) Advisory

Requirement	Priority
The MSP shall advise the CSO on the suitability and potential benefits of utilising existing CSO licences within the cloud environment, where applicable and where relevant to the managed service.	Desired

15 Reporting and Governance

The MSP shall provide structured, accurate and timely reporting to support operational oversight, compliance, service governance and continuous improvement.

Reporting shall be aligned to agreed service levels, contractual obligations and CSO governance requirements and shall reflect the managed service across the existing Landing Zone(s), platform services, in-scope workloads and applications, where applicable.

15.1 Service Level Agreement (SLA) Reporting

Requirement	Priority
The MSP shall provide monthly SLA performance reports covering support services and managed cloud services.	Mandatory
SLA reports shall include response times, resolution times, service availability, performance metrics and any SLA breaches including any agreed enhanced service arrangements applicable during defined peak operational periods.	Mandatory
Reports shall include root cause analysis and remedial actions for any SLA breaches.	Mandatory
SLA reports shall be issued no later than five (5) business days after month-end.	Mandatory
Reports shall include a rolling twelve (12) month performance view.	Mandatory
Ad-hoc SLA reports shall be provided upon reasonable request by the CSO.	Mandatory
SLA reporting shall include, where relevant to the managed service, reporting on incidents, escalations and service actions arising from relevant alerts generated through CSO-operated cloud observability tooling.	Mandatory

15.2 Operational and Technical Reporting

Requirement	Priority
The MSP shall provide regular operational reports covering availability, backup operations, data protection, resilience and capacity including reporting relevant to in-scope workloads and applications where applicable.	Mandatory
Reports shall include backup success rates, schedules, storage utilisation and identified issues or exceptions.	Mandatory
The MSP shall provide capacity and utilisation reporting aligned to Section 10 requirements.	Mandatory
Operational and technical reporting shall include, where relevant to the managed service, reporting on alert trends, operational exceptions and service actions arising from CSO-operated cloud observability tooling.	Mandatory

15.3 Incident and Major Incident Reporting

Requirement	Priority
The MSP shall provide structured incident reports documenting response and recovery activities including, where relevant, incidents arising from or escalated through CSO-operated cloud observability tooling.	Mandatory
For Major Incidents, formal post-incident reports including timelines, impact analysis, root cause and corrective actions shall be provided.	Mandatory

15.4 Business Continuity and Disaster Recovery Reporting

Requirement	Priority
The MSP shall provide reporting on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) performance.	Mandatory
The MSP shall provide reports summarising disaster recovery test outcomes and resilience improvements including any findings relevant to agreed peak operational periods or business-critical windows notified by the CSO.	Mandatory

15.5 Security and Compliance Reporting

Requirement	Priority
The MSP shall provide regular security monitoring reports summarising relevant security events and trends including, where relevant to the managed service, security-related alerts arising from CSO-operated cloud observability tooling.	Mandatory
The MSP shall provide reporting demonstrating compliance with applicable regulatory, contractual and security requirements.	Mandatory
Reports shall include audit outcomes and remediation actions where applicable.	Mandatory
Where UK-based personnel, affiliates or subcontractors are used in the delivery of the managed service, security and compliance reporting shall include confirmation that the approved resource location model remains valid, that any UK-related contingency arrangements remain current, and that any material change affecting the UK's treatment as Nearshore has been notified to the CSO.	Mandatory

15.6 Licence Reporting

Requirement	Priority
The MSP shall provide licence usage and optimisation reports aligned to Section 14.	Mandatory
Licence reports shall include, where relevant, licence status, utilisation, renewals, optimisation opportunities and any material licence-related issues affecting the managed service.	Mandatory

15.7 Trend Analysis and Continuous Improvement

Requirement	Priority
The MSP shall analyse service performance, security, resilience and operational metrics to identify trends and improvement opportunities.	Mandatory
Recommendations for continuous service improvement shall be formally documented and presented during governance meetings.	Mandatory
Trend analysis shall include, where relevant to the managed service, trends arising from recurring alerts, incidents, service exceptions and operational indicators generated through CSO-operated cloud observability tooling.	Mandatory

16 Account and Service Relationship Management

The MSP shall provide structured account and service relationship management to ensure effective governance, communication and continuous alignment with CSO operational and strategic objectives in respect of the managed service from the existing Landing Zone(s) and core platform services through to the in-scope workloads and applications.

16.1 Appointment of Account Manager

Requirement	Priority
The MSP shall appoint a named Account Manager who will act as the primary point of contact for the duration of the contract.	Mandatory
The Account Manager shall be responsible for overall service governance and relationship management including coordination across the managed service from the existing Landing Zone(s) and core platform services through to the in-scope workloads and applications.	Mandatory
All costs associated with account management activities shall be included in the tendered pricing.	Mandatory
The Account Manager shall act as a point of coordination for agreed enhanced service arrangements during defined peak operational periods, where applicable.	Mandatory

16.2 Account Management Responsibilities

Requirement	Priority
The Account Manager shall maintain an effective working relationship with the CSO.	Mandatory
The Account Manager shall oversee service delivery in line with agreed SLAs and contractual obligations including any agreed enhanced service arrangements applicable during defined peak operational periods.	Mandatory
The Account Manager shall ensure appropriate reporting, quality assurance and governance mechanisms are maintained.	Mandatory
The Account Manager shall manage disputes, complaints or service performance concerns.	Mandatory
The Account Manager shall provide regular feedback and recommendations for service improvement and service effectiveness.	Mandatory
The Account Manager shall act as an escalation point for service-related issues.	Mandatory

16.3 Service Review Meetings

Requirement	Priority
The MSP shall participate in formal service review meetings with the CSO, to be held monthly unless otherwise agreed.	Mandatory
Service review meetings shall review SLA performance, incidents, planned changes, upgrades, operational risks and improvement opportunities including, where applicable, service performance during agreed peak operational periods.	Mandatory
The MSP shall present agreed service reports during governance meetings.	Mandatory
Service review meetings shall, where relevant to the managed service, consider recurring alerts, escalations and operational trends arising from CSO-operated cloud observability tooling.	Mandatory

16.4 Operational Engagement

Requirement	Priority
The MSP shall participate in regular operational meetings (e.g. weekly or as otherwise agreed) to address day-to-day service matters including, where relevant, issues arising from CSO-operated cloud observability tooling that relate to the managed service.	Mandatory
Meeting frequency may be adjusted by mutual agreement based on operational demand, including during agreed peak operational periods or where enhanced service arrangements apply.	Mandatory

16.5 Escalation and Dispute Resolution

Requirement	Priority
The MSP shall provide a clearly defined escalation pathway including named contacts, roles and communication channels including escalation arrangements for operational and security events relevant to the managed service.	Mandatory
Escalation pathways shall include 24x7 contact points for critical issues.	Mandatory
The MSP shall cooperate in good faith to resolve disputes in accordance with agreed contractual mechanisms.	Mandatory
The escalation pathway shall support the timely handling and escalation of relevant alerts arising from CSO-operated cloud observability tooling, where such alerts relate to the managed service.	Mandatory

17 Transition and Service Commencement

The MSP shall implement a structured and controlled transition process from the incumbent service provider to ensure continuity of service, risk mitigation and operational stability including the orderly transition into managed service of the existing Landing Zone(s), core platform services, the seven (7) existing in-scope workloads and associated applications.

Continuity of service during transition is mandatory.

17.1 Transition Planning

Requirement	Priority
The MSP shall develop and implement a structured Transition-In Plan prior to service commencement.	Mandatory
The Transition-In Plan shall define scope, timelines, roles, responsibilities and transition milestones.	Mandatory
The Transition-In Plan shall include risk identification and mitigation measures.	Mandatory
The Transition-In Plan shall be subject to CSO review and approval prior to execution.	Mandatory
The Transition-In Plan shall include a defined transition approach for the seven (7) existing in-scope workloads, including workload scope, dependencies, service criticality, current support arrangements and transition sequencing.	Mandatory
The Transition-In Plan shall include the approach to the review, validation and transition of existing infrastructure-as-code artefacts, automation artefacts, repositories, scripts and related configuration items relevant to the managed service.	Mandatory
The Transition-In Plan shall identify transition assumptions, dependencies, required access, documentation requirements and any incumbent cooperation necessary to support successful service commencement.	Mandatory
The Transition-In Plan shall include knowledge capture, knowledge transfer, shadowing and reverse-shadowing activities, where required, to support operational readiness.	Mandatory
The Transition-In Plan shall define service commencement readiness criteria, including validation of monitoring, alert handling, access, escalation pathways, documentation and operational support arrangements.	Mandatory
The Transition-In Plan shall take account of agreed business-critical periods and any enhanced service arrangements required by the CSO during transition and service commencement.	Mandatory

17.2 Knowledge Capture and Handover

Requirement	Priority
The MSP shall conduct structured knowledge capture activities from the incumbent provider including knowledge capture in respect of the existing Landing Zone(s), core platform services, the seven (7) existing in-scope workloads, associated applications, and relevant operational dependencies.	Mandatory
Knowledge transfer activities shall include documentation review, operational briefings and access validation together with review and validation of existing infrastructure-as-code artefacts, automation artefacts, repositories, scripts and related configuration items relevant to the managed service.	Mandatory
Where required, shadowing and reverse-shadowing arrangements shall be implemented to ensure operational readiness including readiness in respect of workload support, monitoring, alert handling, escalation and service continuity arrangements.	Mandatory

17.3 Service Continuity During Transition

Requirement	Priority
The MSP shall ensure no material degradation of service during the transition period including during the transition of the seven (7) existing in-scope workloads and associated applications into the managed service.	Mandatory
The MSP shall maintain operational support coverage throughout transition activities including any agreed enhanced service arrangements applicable during defined peak operational periods.	Mandatory
Any transition-related risks impacting service availability shall be escalated to the CSO immediately including risks relating to access, documentation, incumbent dependency, infrastructure-as-code artefacts, monitoring, alert handling or workload-specific dependencies.	Mandatory

17.4 Service Commencement Readiness

Requirement	Priority
Formal service commencement shall occur only once agreed readiness criteria have been met.	Mandatory
The MSP shall confirm operational readiness including access validation, monitoring validation and process activation prior to go-live together with validation of documentation, alert handling, escalation pathways, operational support arrangements, infrastructure-as-code artefacts relevant to the managed service, and readiness in respect of the seven (7) existing in-scope workloads.	Mandatory

Service commencement readiness shall be demonstrated against agreed criteria approved by the CSO, including confirmation of service continuity, operational handover completion, knowledge transfer completion and support readiness for any agreed peak operational periods.	Mandatory

18 Knowledge Transfer and Capability Enablement

The MSP shall provide structured knowledge transfer, training and documentation to support effective oversight by the CSO Cloud Team and to avoid operational dependency on the MSP in respect of the managed service from the existing Landing Zone(s) and core platform services through to the in-scope workloads and applications.

The objective is to ensure transparency, resilience and capability development within the CSO.

18.1 Ongoing Knowledge Transfer

Requirement	Priority
The MSP shall facilitate structured knowledge transfer sessions with the CSO Cloud Team throughout the contract term.	Mandatory
Knowledge transfer shall include operational processes, architecture overviews, configuration practices and troubleshooting approaches including in relation to the existing Landing Zone(s), core platform services, the seven (7) existing in-scope workloads, associated applications, infrastructure-as-code artefacts, monitoring arrangements, alert handling and escalation processes.	Mandatory
Knowledge transfer activities shall be documented and recorded where appropriate.	Mandatory
Knowledge transfer shall, where relevant, include service arrangements and operational considerations applicable during agreed peak operational periods.	Mandatory

18.2 Training and Skills Enablement

Requirement	Priority
The MSP shall provide ongoing, role-appropriate training aligned to service changes, platform updates and evolving operational requirements including changes affecting the existing Landing Zone(s), platform services, in-scope workloads, applications and operational support model.	Mandatory
Training may include workshops, briefings, technical deep-dives and best-practice sessions including sessions on infrastructure-as-code artefacts, monitoring, alert triage, escalation paths and operational readiness.	Mandatory

Training materials shall be provided in a reusable format accessible to the CSO.	Mandatory

18.3 Documentation Standards

Requirement	Priority
The MSP shall maintain comprehensive, accurate and up-to-date documentation for all managed services including documentation relevant to the existing Landing Zone(s), core platform services, in-scope workloads, associated applications and operational dependencies.	Mandatory
Documentation shall include runbooks, operational procedures, configuration references, automation artefacts and escalation pathways including infrastructure-as-code artefacts and alert handling procedures where relevant to the managed service.	Mandatory
Documentation shall be accessible to the CSO throughout the contract term.	Mandatory

18.4 Avoidance of Single Points of Dependency

Requirement	Priority
The MSP shall ensure that service delivery does not rely on single individuals or undocumented knowledge.	Mandatory
Operational knowledge shall be structured and shareable to support service continuity including continuity in respect of the existing Landing Zone(s), in-scope workloads, associated applications, infrastructure-as-code artefacts and operational support arrangements.	Mandatory

18.5 Cloud Centre of Excellence (Advisory Support)

Requirement	Priority
Where requested, the MSP may provide advisory support to assist the CSO in maturing elements of a Cloud Centre of Excellence (CCoE).	Could
Such advisory support shall focus on operational standards, governance artefacts, knowledge sharing and continuous improvement within the existing cloud environment.	Could

CCoE-related support shall not constitute organisational restructuring or large-scale cloud transformation.	Could

19 Exit and Handover Requirements

Exit readiness shall be maintained throughout the Contract term. The MSP shall ensure that an orderly and controlled transition of services can be executed at contract expiry or termination without disruption to the CSO's operations including in respect of the existing Landing Zone(s), core platform services, the seven (7) existing in-scope workloads, associated applications and relevant operational dependencies.

19.1 Exit and Transition Planning

Requirement	Priority
The MSP shall maintain an up-to-date Exit and Transition Plan throughout the contract term in line with its obligations set out in the Services Agreement.	Mandatory
The Exit Plan shall define activities, timelines, responsibilities and transition dependencies including dependencies relating to the existing Landing Zone(s), core platform services, the seven (7) existing in-scope workloads, associated applications, infrastructure-as-code artefacts and operational support arrangements.	Mandatory
The Exit Plan shall be reviewed periodically and updated to reflect operational changes, in line with the obligations set out in the Services Agreement.	Mandatory
The Exit Plan shall be made available to the CSO upon request.	Mandatory
The Exit Plan shall identify the documentation, access, knowledge transfer, configuration information, infrastructure-as-code artefacts, automation artefacts and service records required to support an orderly transition-out of the managed service.	Mandatory
The Exit Plan shall include arrangements to support continuity of service during transition-out, including during any agreed peak operational periods or business-critical windows notified by the CSO.	Mandatory

19.2 Handover and Collaboration

Requirement	Priority
The MSP shall cooperate fully with the CSO and/or any replacement service provider during transition-out.	Mandatory
The MSP shall provide reasonable assistance to ensure continuity of service during the handover period including continuity in respect of the existing	Mandatory

Landing Zone(s), core platform services, the seven (7) existing in-scope workloads and associated applications.	
The MSP shall not withhold operational knowledge, documentation or access necessary for transition including infrastructure-as-code artefacts, automation artefacts, repositories, scripts, configuration references, runbooks, alert handling procedures and escalation information relevant to the managed service.	Mandatory

19.3 Documentation and Knowledge Transfer

Requirement	Priority
The MSP shall provide up-to-date documentation covering configurations, architecture, automation artefacts, operational procedures and security controls including documentation relevant to the existing Landing Zone(s), core platform services, the seven (7) existing in-scope workloads, associated applications and infrastructure-as-code artefacts.	Mandatory
Documentation shall be sufficient to enable another competent provider to assume responsibility without undue dependency.	Mandatory
Structured knowledge transfer sessions shall be conducted as part of transition-out activities including knowledge transfer in respect of operational support arrangements, alert handling, escalation paths, infrastructure-as-code artefacts and workload-specific dependencies relevant to the managed service.	Mandatory

19.4 Access and Data Continuity

Requirement	Priority
The MSP shall ensure all access credentials, configurations and service artefacts remain under CSO control at contract expiry including infrastructure-as-code artefacts, automation artefacts, repositories, scripts and related configuration items relevant to the managed service.	Mandatory
The MSP shall not restrict, disable or otherwise impede CSO access to its cloud environment upon termination.	Mandatory
All CSO data shall remain within CSO-controlled accounts and environments.	Mandatory

19.5 Commercial Transparency and Exit Costs

Requirement	Priority
Tenderers shall clearly state any costs associated with exit and transition support in their pricing submission.	Mandatory
Any exit-related costs shall be transparent, pre-defined and proportionate to the support required including any costs associated with transition-out support for the existing Landing Zone(s), core platform services, the seven (7) existing in-scope workloads and associated applications.	Mandatory
The MSP shall not impose additional charges beyond those disclosed and agreed within the contract.	Mandatory

19.6 Cloud Service Provider (CSP) Wind-Down Support

Requirement	Priority
Where a change of managed service provider is required, the MSP shall support wind-down and transition activities relating to the managed services including activities relating to the existing Landing Zone(s), core platform services, the seven (7) existing in-scope workloads, associated applications and relevant operational dependencies.	Mandatory
Transition activities shall not adversely impact service continuity, data integrity or security including during any agreed peak operational periods or business-critical windows notified by the CSO.	Mandatory
The MSP shall not commit the CSO to any commercial or contractual obligations with AWS or other vendors during transition-out without written authorisation.	Mandatory

20 Relationship with Amazon Web Services (AWS)

The CSO shall retain the contractual relationship with Amazon Web Services (AWS) for the provision of hyperscale cloud services.

The MSP shall operate strictly within the parameters defined below.

20.1 Contractual Relationship with AWS

Requirement	Priority
The MSP shall not be a contractual party to the CSO's AWS agreements.	Mandatory
The MSP shall have no authority to negotiate, amend or commit to AWS commercial terms on behalf of the CSO.	Mandatory
The MSP shall not enter into financial, commercial or contractual obligations with AWS without explicit written authorisation from the CSO.	Mandatory

20.2 Operational Interface with AWS

Requirement	Priority
The MSP shall act as the primary operational interface with AWS for the purposes of service delivery in respect of the managed service including the existing Landing Zone(s), core platform services, in-scope workloads and associated applications where applicable.	Mandatory
The MSP shall raise, manage and coordinate AWS Support cases on behalf of the CSO.	Mandatory
The MSP shall engage with AWS technical support during incidents, including Major Incidents.	Mandatory
The MSP shall coordinate implementation of AWS-recommended remediations, subject to CSO change and approval processes.	Mandatory
The MSP shall coordinate incident resolution activities involving AWS services.	Mandatory

20.3 Governance and Control

Requirement	Priority
All engagement with AWS shall be conducted in accordance with CSO-defined governance, security and change management controls.	Mandatory

The MSP shall ensure transparency of all AWS-related communications relevant to the managed services.	Mandatory
The MSP shall not use its operational interface role with AWS to assume or imply any commercial, contractual, FinOps or budgetary authority, all of which shall remain solely with the CSO.	Mandatory

20.4 AWS Commercial Value Advisory Support

Requirement	Priority
The MSP shall use its AWS partner status, programme participation and support relationships to identify and evidence potential AWS commercial benefits, credits, funding, discounts, optimisation opportunities or incentives that may be available to the CSO. The MSP shall support the CSO in assessing and pursuing such opportunities, but shall not commit the CSO to any AWS commercial, contractual or financial obligation without the CSO's prior written approval. FinOps, AWS commercial decision-making and budgetary control shall remain with the CSO.	Mandatory

21 Out-of-Scope Services

The following services and responsibilities are explicitly excluded from the scope of this Contract.

The managed service under this Contract is limited to the ongoing operational management, support and optimisation of the CSO's existing cloud environment and associated in-scope services. For the avoidance of doubt, the following services, responsibilities and activities are outside the scope of the managed service unless expressly provided for elsewhere in this Appendix or separately agreed in writing through a formal change control or Statement of Work process.

- Hyperscaler procurement or resale.
- AWS commercial contract management.
- Cloud strategy definition.
- Initial landing zone design and build.
- FinOps ownership or budgetary control.
- Ownership of environments, data, or IP.
- Cloud financial governance, budgeting and commercial decision-making.
- Ownership or operation of the CSO's cloud observability capability.
- Redesign, rebuild or large-scale transformation of the underlying cloud platform.
- Organisational restructuring or large-scale cloud transformation activity.