Important Note: 21 July 2026
References in tenderer queries to the original Section 12 or to individual subsections of the original Section 12 should be read in light of Appendix 1 Part B v4.1. Revised Section 12 supersedes the original Section 12 and the SOC, SIEM and cyber-security operations requirements in Section 6.3 to the extent stated in revised Section 12

No.	Query	Response
2	We have noted a similar requirement was awarded in 2024 with a budget of €2m with a 2+1+1 term. Can you confirm the following please: Why were the optional extensions not taken? Why has the budget grown from €2m to €10m? Given we are approaching the summer holiday period with many people starting annual leave, the value of the contract and the submission required, is it possible to grant an extension to the response deadline? Otherwise we may have decline to respond for capacity reason, despite our strong interest to bid.	The previous arrangement related to a different scope of services and delivery phase and was not considered the appropriate long-term vehicle for the requirement now being procured. The estimated contract value for this Competition reflects the full potential contract term, the ongoing managed-service scope and potential separately commissioned project activity. Tenderers should prepare their Tenders solely on the basis of the current procurement documents.
3	We have some further follow up questions: Can you confirm if TUPE or equivalent applies to this contract? Could you kindly come back to us regarding the extension request please, given current resourcing and holiday commitments we estimate 20 working days being required.	TUPE or equivalent arrangements do not apply to this Contract. The clarification and tender submission deadlines have been extended. Please refer to the separate clarification and updated eTenders notice for details.
4	To assist tenderers in accurately sizing and pricing the managed service, could the Contracting Authority provide indicative high-level AWS estate metrics, such as: • Number of AWS accounts • Approximate monthly AWS spend (or spend band) • Number of in-scope workloads/environments • Indicative scale of AWS resources (e.g. EC2, RDS, EKS and storage footprint) High-level ranges would be acceptable if exact figures cannot be disclosed. same	The following figures represent an indicative point-in-time snapshot of the AWS estate and may change during the procurement and Contract term. Tenderers should clearly state any material sizing assumptions used in preparing their Tender. Approximate monthly AWS spend (or spend band) €40 - €55,000 monthly. • 7 Workloads AWS Regions - Ireland (eu-west-1) - Frankfurt (eu-central-1) - us-east-1 (billing etc) An indicative list of AWS Services Breakdown • Accounts — 26 • RDS — 11 (10 active) • DynamoDB — 3 (VDR + Root Account) • EC2 — 63 • Accounts with SES — 2 • Site to Site VPNS - 2 • Shared Cloud Resources (Accounts) — 9 • Storage Services in use — 8 (EBS, S3, RDS, FSx, EFS, DynamoDB, Glacier, Backup) • Total Storage (GB-Month) — 14,627 GB EC2 in accounts (DEV, PROD, UAT) • Census Recruitment – 11 EC2 • Census Website – 0 • Census Hub – 3 • Blaise – 4 • PXSTAT – 14 • Innovation Hub – 2 • VDR – 25 • Shared Cloud Resources – 4 RDS in accounts (DEV, PROD, UAT) • Census Recruitment – 3 • Census Website – 0 • Census Hub – 1 • Blaise – 0 • PXSTAT – 3 • Innovation Hub – 2 • VDR – 2 • Shared Cloud Resources – 0 Serverless Services in use (no. of accounts) • Lambda — 26 • SES — 2 • SNS — 26 • SQS — 26 • DynamoDB — 3 (VDR + Root Account) Security Services (no. of accounts) • AWS Shield Advance — 1 (root) • AWS Network Firewall — 1 (shared networks account)

		• AWS WAF — 14 (Web ACLs) • Amazon GuardDuty — 26 Governance Services (no. of accounts) • AWS Directory Service — 11 • CloudTrail — 25 • KMS — 26 • CloudWatch — 24 • Config — 26 • Cost Explorer — 1 • CodeBuild — 1 • CodeArtifact — 1 • AWS Backup — 1 Storage Services (no. of accounts, total GB-month) • FSx — 6 accounts — 203.1GB • S3 — 23 accounts — 2556.9 GB • EFS — 5 accounts — 0.8 GB • EBS (Volumes + Snapshots) — 16 accounts — 9591.5 GB • RDS — 10 accounts — 2271.5 GB • AWS Backup (EFS warm storage) — 3 accounts — 2.91 GB • DynamoDB — 3 accounts — 0 GB • Glacier — 5 accounts — 0 GB Networking Services (no. of accounts) • VPC — 14 • Amazon ELB — 12 • Amazon Route 53 — 4 (VDR) • Amazon Kinesis — 3 (VDR + LogArchive) • Amazon Firehose — 1 (Log Archive account) Instance types and count (63 in total) • t3.medium — 14 • r6i.2xlarge — 9 • t3.large — 8 • m5.large — 6 • t3a.xlarge — 3 • t3.2xlarge — 3 • m5.xlarge — 3 • r6i.large — 4 • t2.micro — 2 • t3a.large — 2 • c5.large — 2 • m6a.2xlarge — 2 • t3.xlarge — 2 • t3.small — 1 • r5.xlarge — 1 • m5a.xlarge — 1 RDS Instance Types and count (11 in total) • db.r6i.2xlarge — 5 • db.m6i.xlarge — 3 • db.r5.xlarge — 1 • db.r5.large — 1 • db.r6i.xlarge — 1
5	Service Desk Volume (Section 4.5 – Current Service Desk Ticket Volumes): Can the CSO provide a monthly breakdown of ticket volumes by classification (Incident, Service Request, Change, Problem, Access Request, Security Event) for the last 12 months? Can the CSO provide historical monthly change volumes split by standard, normal Can the CSO provide historical problem records and recurring incident trends for the existing environment?	The information currently available is the aggregate historic ticket volume stated in Section 4.5. A reliable monthly breakdown across all requested classifications, historic change categories and problem trends is not available in a consistent format. Tenderers should base their proposals on the information published in the RFT and clearly state any reasonable assumptions. The figures are indicative and do not constitute a guaranteed minimum or maximum volume. Variance from a Tenderer assumption will not of itself give rise to an automatic adjustment of the managed-service fee.
6	Service Desk Volume (Section 4.5): Can the CSO provide a breakdown of tickets by workload/application and by support tier (L1/L2/L3)?	Based on the available historic service-desk records, no incidents or service requests logged directly by CSO staff during the referenced period were raised outside standard business hours. This does not include monitoring-generated alerts, SOC activity or incidents identified proactively by the MSP outside business hours. From Aug 2025 to Apr 2026 the following tickets were raised: Censushub/Colectica 11 (10 = P3 and 1 = P2), CSO PxStat 64 (6 = P1, 2 = P2, 49 = P3, 6 = P4 and 1 = Lowest), CSO Blaise 12 (12 = P3), Shared Networks 2 (2 = P3), Other CMS General Works 52 (1 =P1, 3 = P2, 47 = P3 and 1 = P4).
7	Service Desk Channels (Section 6.3 Service Desk and Operational Support): Which channels are expected for service engagement (portal, email, telephone, chat, Teams integration, API, mobile)?	The service desk must support, at a minimum, portal/web access, email and telephone channels, together with appropriate 24x7 on-call and escalation arrangements. Any additional channels, integrations or APIs proposed by the Tenderer may be considered where they support the service requirements and comply with CSO security and governance controls.

8	Service Desk Users (Section 6.3): Approximately how many named users are expected to access the service desk, including CSO staff and approved third parties?	A definitive named-user count is not available. The service desk will be used primarily by authorised CSO technical and service-management contacts, application owners and approved third parties and is not intended to operate as a general end-user helpdesk for all CSO personnel. Tenderers should include sufficient user access and licensing to support this operating model and shall clearly state any named-user or licensing assumptions used in preparing their Tender.
9	Service Desk Scope (Section 6.3 and Section 11.1): Is the successful bidder expected to provide direct end-user support for application issues relating to PxStat, Blaise, VDR, Colectica, Census Hub and Census applications, or only cloud infrastructure and platform support?	The successful Tenderer will provide operational support for the in-scope cloud platform, workloads, application runtime, configuration and relevant service dependencies, including incident coordination with CSO teams and third-party application suppliers. The scope does not include general business-user functional support, application development or material code changes unless expressly agreed through a Statement of Work or formal change control process.
10	Service Levels (Section 6.3): Can the CSO provide the full incident severity definitions for P1, P2, P3 and P4	The CSO has not prescribed a detailed P1–P4 incident classification model for tender purposes. Tenderers should provide their proposed incident severity model, including: • impact and urgency criteria; • indicative incident examples; • response and restoration or resolution targets; • escalation arrangements; and • communication requirements. The proposed model must support the 24x7x365 management of P1 and P2 incidents. P3 and P4 incidents will normally be managed during the applicable agreed service hours unless otherwise required for a particular workload, peak operational period or business-critical window The final severity definitions, targets and associated procedures will be agreed with the successful Tenderer during mobilisation and will remain subject to CSO approval.
11	Service Levels (Section 6.3): Are response and resolution targets measured 24x7 or during agreed support windows for each priority?	The service must support the management of P1 and P2 production and security incidents on a 24x7x365 basis. P3 and P4 incidents will normally be managed during the applicable agreed service hours unless otherwise specified for a workload, peak operational period or business-critical window. The detailed response, restoration and resolution targets for each priority will be based on the successful Tenderer's proposed service-level model and finalised during mobilisation, subject to CSO approval.
12	Service Desk Tooling (Section 6.3): Are there specific ITSM platforms currently in use by the CSO (e.g. ServiceNow, Jira Service Management, Freshservice)?	The successful Tenderer shall provide, host, license, configure, operate, maintain and support the IT Service Management platform required to deliver the managed service. The incumbent provider's ticketing platform will not transfer to the new Contract. The proposed ITSM platform must support the required incident, problem, change, request, knowledge, reporting, audit, access-control, data-export and integration capabilities. All associated costs shall be included in the Tender unless expressly identified and priced in accordance with the Costs Schedule.
13	Knowledge Management (Section 18): Does the CSO currently maintain a knowledge base and is the successful bidder expected to create and maintain user-facing knowledge articles?	Existing operational documentation, runbooks and knowledge material will be made available to the successful Tenderer during transition where available. The MSP will be required to validate, maintain and improve service knowledge, operational runbooks and support documentation throughout the contract. User-facing knowledge articles are required only where agreed as relevant to the managed service; the requirement is not for a general CSO end-user knowledge base.
14	Governance (Sections 7, 15 and 16): Can the CSO provide its expected governance calendar, forum structure and attendee profiles (operational, tactical and executive)?	The CSO's current governance model includes:• weekly operational support meetings with relevant CSO stakeholders;• quarterly service review meetings; and • biannual strategic review meetings. The weekly operational meeting is expected to focus on current incidents, service requests, problems, changes, security matters, monitoring alerts, planned maintenance, operational risks, outstanding actions and upcoming workload or business events. Attendees would normally include the MSP Service Delivery Manager and relevant operational and technical representatives from the MSP and CSO. The quarterly service review is expected to consider overall service performance, SLA and KPI achievement, incident and problem trends, security and vulnerability management, capacity, resilience, disaster recovery, FinOps, service improvement, risks, supplier performance and the forward service plan. Attendees would normally include the MSP Service Delivery Manager, relevant technical leads and the appropriate CSO service, architecture, security and management representatives. Tenderers should propose a governance structure and meeting cadence that meets or exceeds these requirements. The proposal should identify the purpose, frequency, attendees, reporting inputs, decision-making responsibilities, escalation routes, action tracking and expected outputs for each forum Tenderers should propose a governance structure and meeting cadence that meets or exceeds these requirements.
15	Security Operations Boundary (Sections 6.3 and 12): The specification references both an successful bidder-provided SOC and an existing CSO-contracted SOC. Can the CSO clarify the division of responsibilities between these parties?	The incoming MSP has end-to-end operational responsibility for the AWS SOC/SIEM service. The on-premises SOC/SIEM remains outside scope, with coordination required where events or incidents cross environments. Refer the Tenderer to revised Section 12 of Appendix 1 Part B v4.1 of Appendix 1 for the detailed requirements.
16	Security Ticket Flow (Sections 6.3 and 12): Will security incidents be logged and managed through the successful bidder service desk tool, the CSO SIEM workflow, or a combination of both?	Security alerts will be generated, correlated, triaged and investigated through the successful Tenderer's SOC and SIEM service. Where an alert meets the agreed incident-classification threshold, it shall be recorded and managed as a security incident in the Tenderer's ITSM platform. CSO shall be notified and incidents shall be escalated in accordance with the agreed severity model, notification thresholds, communication procedures and incident-response runbooks. Where an incident spans AWS and another CSO environment, coordination will take place through service-desk tickets, notifications, calls and agreed escalation routes. Direct integration with the on-premises SIEM is not required unless separately agreed.
17	Change Management (Section 9): Is there an existing CAB structure and change approval workflow that the successful bidder must adopt, or is the successful bidder expected to provide this capability?	CSO retains approval authority for material changes to the AWS environment. The successful Tenderer shall provide and operate the change-management process and supporting tooling in accordance with the RFT.
18	Configuration Management (Section 7.3):	The CSO maintains relevant asset, configuration, architecture and service information, although no specific CMDB product is mandated in the RFT. The successful Tenderer will be required to maintain accurate configuration and service records in the agreed repositories and to support any required integration or reconciliation with CSO records. **The detailed repository and tooling arrangements will be confirmed during transition**

	Does the CSO maintain an existing CMDB or asset repository and is the successful bidder expected to update it?	
19	Incumbent Contract (Section 17): What is the current incumbent contract end date and what overlap period is anticipated with the incoming provider?	The current MSP arrangement is being extended to maintain service continuity through the procurement and transition period. The Contracting Authority anticipates an appropriate overlap with the incoming provider to support knowledge transfer, shadowing, handover and service continuity.
20	Transition (Section 17): Can the CSO provide the anticipated transition duration between contract award and service commencement?	Tenderers should propose a realistic transition approach and indicative timeframe addressing: • mobilisation; • access provisioning; • knowledge transfer; • documentation validation; • shadowing and reverse-shadowing where appropriate; • operational readiness; • service handover; and • continuity of service. The final transition duration, sequencing, milestones and responsibilities will be agreed with the successful Tenderer and the incumbent provider as part of the Transition-In Plan, subject to CSO approval.
21	Third-Party Management (Sections 4.6 and 20): Can the CSO provide a list of major third parties with whom the successful bidder will be expected to coordinate (AWS, Datadog, development partners, call centre providers, application vendors, etc.)?	The successful Tenderer will be expected to coordinate, where relevant to the managed-service scope, with the CSO's internal teams and a range of third-party service providers. These may include: • AWS; • Datadog and Pingdom; • application development, maintenance and support providers; • network, telecommunications and connectivity providers; • cybersecurity, penetration-testing and assurance providers;• workload-specific software vendors; and • the incumbent MSP during transition. This list is indicative and not exhaustive, as third-party providers may change during the contract term. The successful Tenderer will be expected to act as the primary operational coordinator for incidents, problems, changes, service dependencies and escalations relating to the managed-service scope. This will include maintaining relevant contact and escalation details, coordinating technical investigations, supporting joint service reviews and tracking actions through to resolution.
22	Current Service Model (Sections 4.6 and 17): Can the CSO provide a high-level view of the current support organisation, including retained CSO resources, incumbent resources and third-party suppliers?	The current operating model is based on retained CSO strategic control with managed service provider support for day-to-day cloud operations. At a high level, the CSO retains responsibility for cloud governance, AWS commercial management, FinOps, architecture and security approval controls, the CSO-owned observability capability, and overall service direction. CSO application, cloud and cybersecurity teams remain involved as required in relation to application ownership, governance, escalation, approval and oversight. The managed service provider is responsible for day-to-day operational support of the in-scope cloud environment, including incident coordination, service desk interaction, operational monitoring response, support, maintenance, reporting and coordination with relevant CSO teams, AWS and third-party suppliers where required. Third-party suppliers may be involved in relation to underlying cloud services, observability/tooling, application support or other service dependencies. Tenderers should base their responses on the operating model, retained responsibilities, in-scope workloads, service management, transition and governance requirements set out in Appendix 1: Part B of the RFT. The CSO is not providing details of the incumbent provider's internal resourcing model, personnel, commercial arrangements or supplier-specific operating structure. Tenderers should propose their own support organisation and delivery model capable of meeting the requirements set out in the tender documents.
23	TUPE Applicability (Section 2.11.2): Is TUPE expected to apply and will ELI be provided?	TUPE or equivalent arrangements do not apply to this contract.
24	Workload Growth (Section 11.6): Can the CSO provide an indicative roadmap of planned new workloads expected during the contract term?	No committed or guaranteed roadmap of future workloads is being provided. The CSO expects that new or amended workloads may be introduced during the contract term, including workload activity associated with major statistical programmes and evolving business requirements. Such workloads will be onboarded through the governance, change-control and Statement of Work mechanisms set out in the RFT. The stated contract value and person-day estimates are indicative only and do not guarantee volume.
25	Service Baseline (Section 4 Current Environment): Can the CSO provide sizing information including AWS account count, server count, databases, storage volumes, VPNs and active workloads?	The following figures represent an indicative point-in-time snapshot of the AWS estate and may change during the procurement and Contract term. Tenderers should clearly state any material sizing assumptions used in preparing their Tender. Approximate monthly AWS spend (or spend band) €40 - €55,000 monthly. • 7 Workloads AWS Regions - Ireland (eu-west-1) - Frankfurt (eu-central-1) - us-east-1 (billing etc) An indicative list of AWS Services Breakdown

• Accounts — 26
• RDS — 11 (10 active)
• DynamoDB — 3 (VDR + Root Account)
• EC2 — 63
• Accounts with EC2 — 15
• Accounts with Lambda — 26
• Accounts with SES — 2
• Site to Site VPNS - 2
• Shared Cloud Resources (Accounts) — 9
• Storage Services in use — 8 (EBS, S3, RDS, FSx, EFS, DynamoDB, Glacier, Backup)
• Total Storage (GB-Month) — 14,627 GB

EC2 in accounts (DEV, PROD, UAT)
• Census Recruitment – 11 EC2
• Census Website – 0
• Census Hub – 3
• Blaise – 4
• PXSTAT – 14
• Innovation Hub – 2
• VDR – 25
• Shared Cloud Resources – 4

RDS in accounts (DEV, PROD, UAT)
• Census Recruitment – 3
• Census Website – 0
• Census Hub – 1
• Blaise – 0
• PXSTAT – 3
• Innovation Hub – 2
• VDR – 2
• Shared Cloud Resources – 0

Serverless Services in use (no. of accounts)
• Lambda — 26
• SES — 2
• SNS — 26
• SQS — 26
• DynamoDB — 3 (VDR + Root Account)

Security Services (no. of accounts)
• AWS Shield Advance — 1 (root)
• AWS Network Firewall — 1 (shared networks account)
• AWS AWS Security Hub — 26
• AWS WAF — 14 (Web ACLs)
• Amazon GuardDuty — 26

Governance Services (no. of accounts)
• AWS Directory Service — 11
• CloudTrail — 25
• KMS — 26
• CloudWatch — 24
• Config — 26
• Cost Explorer — 1
• CodeBuild — 1
• CodeArtifact — 1
• AWS Backup — 1

Storage Services (no. of accounts, total GB-month)
• FSx — 6 accounts — 203.1GB
• S3 — 23 accounts — 2556.9 GB
• EFS — 5 accounts — 0.8 GB
• EBS (Volumes + Snapshots) — 16 accounts — 9591.5 GB
• RDS — 10 accounts — 2271.5 GB
• AWS Backup (EFS warm storage) — 3 accounts — 2.91 GB
• DynamoDB — 3 accounts — 0 GB
• Glacier — 5 accounts — 0 GB

Networking Services (no. of accounts)
• VPC — 14
• Amazon ELB — 12
• Amazon Route 53 — 4 (VDR)
• Amazon Kinesis — 3 (VDR + LogArchive)
• Amazon Firehose — 1 (Log Archive account)

Instance types and count (63 in total)
• t3.medium — 14
• r6i.2xlarge — 9
• t3.large — 8
• m5.large — 6
• t3a.xlarge — 3
• t3.2xlarge — 3
• m5.xlarge — 3
• r6i.large — 4
• t2.micro — 2
• t3a.large — 2

		• c5.large — 2 • m6a.2xlarge — 2 • t3.xlarge — 2 • t3.small — 1 • r5.xlarge — 1 • m5a.xlarge — 1 RDS Instance Types and count (11 in total) • db.r6i.2xlarge — 5 • db.m6i.xlarge — 3 • db.r5.xlarge — 1 • db.r5.large — 1 • db.r6i.xlarge — 1
26	Support Coverage (Sections 6.3 and 4.2): Are all seven existing workloads expected to be supported from service commencement, or is phased onboarding anticipated?	All existing in-scope workloads identified in Appendix 1 are included within the managed-service scope. Transition activities may be sequenced on a workload-by-workload basis, but the incoming MSP is expected to assume responsibility for the full in-scope service by completion of the agreed transition period.
27	Retained Team (Section 4.6): Can the CSO provide details of the retained cloud, security and service management teams that will interface with the MSP?	The retained CSO interface will include Cloud Services management and operations, cloud architecture, cybersecurity, network and infrastructure, service management, application owners and relevant Data Office, Finance/FinOps and Procurement stakeholders. Exact named resources and detailed attendance arrangements may change over the term and will be confirmed through mobilisation and governance. Tenderers should propose a delivery model capable of interfacing effectively with this retained organisation.
28	RACI (Section 7.1): Can the CSO provide an indicative RACI between CSO teams, the MSP, application owners and other service providers?	The CSO will retain overall governance, decision-making and approval authority for the AWS environment, including architecture, security, risk acceptance, financial governance, access approval and material change approval. The successful Tenderer will be responsible for the operational delivery and coordination of the managed service, including monitoring, incident and problem management, change implementation, patching, backup and recovery operations, SOC activities, service reporting and coordination with relevant third parties. Application owners will retain responsibility for application-level business priorities, functional decisions, business-impact assessment, user acceptance testing and approval of application releases or changes where applicable. Other service providers will remain responsible for the products and services within their respective contractual scope. The successful Tenderer will be expected to coordinate operational activities, escalations and dependencies with those providers but will not assume responsibility for matters outside its contracted scope. A detailed service RACI, including escalation routes, approval thresholds and interfaces between the CSO, the successful Tenderer, application owners, AWS and other providers, will be finalised during mobilisation and will remain subject to CSO approval.
29	AI (N/A): What is CSO current 'Use of AI policy' for productivity, code generation, workflow automation, access to data and environments and GenAI tooling such as cursor? If there is no formal policy than what is likely inclination or appetite towards to agentic autonomous operations with sufficient human oversight?	Tenderers must not assume unrestricted use of generative AI, autonomous agents or public AI services in delivering the managed service. Any proposed use of GenAI, AIOps, code-generation or agentic tooling will require prior written CSO approval and must comply with CSO security, data-protection, confidentiality, records-management and change-control requirements.
30	Contract (N/A): Any urgency related time or contractual constraints that may impact the need to switch incumbents? (EOT, EOL)	The CSO is not aware of any specific end-of-life, end-of-support or technology-driven urgency issue that requires an accelerated transition. This Competition has been initiated because the existing contractual arrangements for the relevant services have reached the end of their available term and/or value. In accordance with public procurement requirements, the CSO is therefore conducting a new competitive process for the services described in the tender documents. For the avoidance of doubt, the CSO is conducting an open procedure and has no preferred supplier. All Tenders will be evaluated in accordance with the Selection and Award Criteria set out in the RFT.
31	Contract (N/A): SLA Commitment: Do infrastructure require active operations 24x7? Are all application support required 24x7? Do any or all applications requirement zero down time releases? Are there any specific KPIs for service improvements and optimisation over time already defined or tracked for the current incumbent? What are defined SLA for Out of hours operations and Services, Are there any releases out of hours requirements?	The managed service must provide 24x7x365 monitoring, alerting and operational response for the AWS infrastructure, platform services, security events and P1/P2 incidents. Not all application support is required on a 24x7 basis. P3/P4 incidents and routine operational activities will normally be managed during the applicable agreed service hours, unless a workload, critical processing period or business event requires extended support. The MSP's responsibility is primarily for the managed cloud platform and infrastructure; application-functional support remains with the relevant application owner or third-party provider unless expressly included in scope. Zero-downtime releases are not a universal requirement. Tenderers should propose deployment and maintenance approaches that minimise disruption and support high availability where required. Release methods and permitted downtime will be agreed on a workload-by-workload basis, taking account of business criticality, architecture and operational requirements. Out-of-hours releases or maintenance may be required for production services, security remediation, major changes, critical processing periods and other business-sensitive activities. These will be planned through the agreed change and release-management process. Tenderers should propose appropriate KPIs for service improvement and optimisation, including service availability, incident trends, problem reduction, automation, capacity, resilience, security, cost optimisation and continuous improvement. The final KPI set, baselines and improvement targets will be agreed with the successful Tenderer during mobilisation, subject to the minimum requirements in the RFT and CSO approval
32	Operating Model (N/A): Could you share your perspective on current levels of engagement within engineering operating model across SDLC (App teams, platform owner, business, finance, procurement, architecture) - in stages of Architecture, Design, Roadmap, Engineering, Release Planning, Transition to support, Change impact, communication.	CSO application teams generally retain responsibility for business requirements, application design, software development, testing and application-level release decisions. CSO Cloud Services is the AWS platform owner and retains responsibility for cloud governance, operational oversight, service acceptance, change approval, security coordination and management of the MSP relationship. CSO Architecture retains responsibility for architectural governance and standards. The successful Tenderer will provide operational and technical input throughout the relevant delivery lifecycle, including architecture and design, infrastructure provisioning, networking, security controls, automation, monitoring, release planning, operational-readiness assessment and transition to support.

		Application teams will normally consume standard AWS infrastructure and platform services, including EC2 and RDS. AWS platform activities such as account provisioning, networking, access configuration, autoscaling, monitoring and platform operations will generally be undertaken by the MSP through the applicable BAU ticket, change-control or Statement of Work process. The detailed RACI, engagement model, governance forums and approval points will be agreed during mobilisation
33	Architecture & Environments (Appendix 1, Part B, Section 4 & 4.1): To help us build a highly accurate baseline for the managed service, could the CSO permit tenderers to review the existing LZA configuration files during the tender period, and kindly provide an indicative numerical count of AWS accounts, servers, databases, storage volumes, and active workloads? If this documentation and data cannot be provided at this stage, would the CSO be agreeable to tenderers stating their own baseline volume and configuration assumptions in the Pricing Schedule, with the understanding that significant variations at service commencement can be managed collaboratively via Change Control?	The Contracting Authority will not provide Tenderers with access to the detailed LZA configuration repositories during the tender period. We are currently running the AWS LZA version 1.14.5 The following figures represent an indicative point-in-time snapshot of the AWS estate and may change during the procurement and Contract term. Tenderers should clearly state any material sizing assumptions used in preparing their Tender. Approximate monthly AWS spend (or spend band) €40 - €55,000 monthly. • Approximate monthly AWS spend (or spend band) €40 - 55,000 monthly • 7 Workloads AWS Regions - Ireland (eu-west-1) - Frankfurt (eu-central-1) - us-east-1 (billing etc) An indicitive list of AWS Services Breakdown • Accounts — 26 • RDS — 11 (10 active) • DynamoDB — 3 (VDR + Root Account) • EC2 — 63 • Accounts with EC2 — 15 • Accounts with Lambda — 26 • Accounts with SES — 2 • Site to Site VPNS - 2 • Shared Cloud Resources (Accounts) — 9 • Storage Services in use — 8 (EBS, S3, RDS, FSx, EFS, DynamoDB, Glacier, Backup) • Total Storage (GB-Month) — 14,627 GB EC2 in accounts (DEV, PROD, UAT) • Census Recruitment – 11 EC2 • Census Website – 0 • Census Hub – 3 • Blaise – 4 • PXSTAT – 14 • Innovation Hub – 2 • VDR – 25 • Shared Cloud Resources – 4 RDS in accounts (DEV, PROD, UAT) • Census Recruitment – 3 • Census Website – 0 • Census Hub – 1 • Blaise – 0 • PXSTAT – 3 • Innovation Hub – 2 • VDR – 2 • Shared Cloud Resources – 0 Serverless Services in use (no. of accounts) • Lambda — 26 • SES — 2 • SNS — 26 • SQS — 26 • DynamoDB — 3 (VDR + Root Account) Security Services (no. of accounts) • AWS Shield Advance — 1 (root) • AWS Network Firewall — 1 (shared networks account) • AWS AWS Security Hub — 26 • AWS WAF — 14 (Web ACLs) • Amazon GuardDuty — 26 Governance Services (no. of accounts) • AWS Directory Service — 11 • CloudTrail — 25 • KMS — 26 • CloudWatch — 24 • Config — 26

		• Cost Explorer — 1 • CodeBuild — 1 • CodeArtifact — 1 • AWS Backup — 1 Storage Services (no. of accounts, total GB-month) • FSx — 6 accounts — 203.1GB • S3 — 23 accounts — 2556.9 GB • EFS — 5 accounts — 0.8 GB • EBS (Volumes + Snapshots) — 16 accounts — 9591.5 GB • RDS — 10 accounts — 2271.5 GB • AWS Backup (EFS warm storage) — 3 accounts — 2.91 GB • DynamoDB — 3 accounts — 0 GB • Glacier — 5 accounts — 0 GB Networking Services (no. of accounts) • VPC — 14 • Amazon ELB — 12 • Amazon Route 53 — 4 (VDR) • Amazon Kinesis — 3 (VDR + LogArchive) • Amazon Firehose — 1 (Log Archive account) Instance types and count (63 in total) • t3.medium — 14 • r6i.2xlarge — 9 • t3.large — 8 • m5.large — 6 • t3a.xlarge — 3 • t3.2xlarge — 3 • m5.xlarge — 3 • r6i.large — 4 • t2.micro — 2 • t3a.large — 2 • c5.large — 2 • m6a.2xlarge — 2 • t3.xlarge — 2 • t3.small — 1 • r5.xlarge — 1 • m5a.xlarge — 1 RDS Instance Types and count (11 in total) • db.r6i.2xlarge — 5 • db.m6i.xlarge — 3 • db.r5.xlarge — 1 • db.r5.large — 1 • db.r6i.xlarge — 1
34	Architecture & Environments (Appendix 1, Part B, Section 4.1): Could the CSO provide further detail on whether the MSP will have exclusive management responsibility for the "DevOps Automation" account, while the CSO retains management of the "Platform Automation" account? If this is not the case, could the CSO outline the preferred operational boundaries and tooling demarcation between the two central accounts to ensure we propose the most effective engagement model?	The Platform Automation account supports landing-zone and infrastructure automation. The DevOps Automation account supports application-code deployment workflows. Under the current model, the MSP operates both accounts and performs deployments to UAT and production after CSO application teams provide the approved code or deployment artefacts. CSO application teams may perform development-environment deployments.
35	Architecture & Environments (Appendix 1, Part B, Section 4.1): To ensure we propose the most suitably certified network engineering personnel, could the CSO confirm the underlying technology and vendor for the central firewall? If the solution relies on a third-party virtual appliance (e.g., Palo Alto, Fortinet), could the CSO advise whether it maintains the licensing, or if tenderers should incorporate these subscription costs into their fixed recurring fee?	The central firewall capability uses AWS Network Firewall and does not rely on a third-party virtual firewall appliance
36	Architecture & Environments (Appendix 1, Part B, Section 4 (Architecture Diagrams)): To assist with our firewall capacity planning, could the CSO clarify whether internal East/West traffic (VPC-to-VPC communication) is also routed through the central firewall for inspection? If this operational detail is currently unavailable, may we kindly assume for scoping purposes that only North/South (Ingress/Egress) inspection is required for the fixed-fee component?	We follow standard LZA setup, so all traffic is inspected.
37	Architecture & Environments (Appendix 1, Part B, Section 6.3): To ensure we can confidently commit to the 4-hour P1 resolution targets, could the CSO confirm whether the critical in-scope workloads are currently deployed in a Highly Available (HA) configuration? If the current architecture is not natively HA, would the CSO consider relaxing the SLA resolution target for those specific workloads until such time as they are upgraded, to ensure a fair and balanced risk profile?	All applications in all environments are to be supported in line with agreed resolution times. There are currently no plans to make any changes to workloads/environments that are not currently HA. The successful Tenderer will be required to support the estate as deployed at service commencement and meet the applicable incident-management requirements.
38	Architecture & Environments (Appendix 1, Part B, Section 4.2): Noting the varying environment structures currently in place (e.g., Colectica operating solely in Production, while Blaise and VDR use Dev/UAT/Prod), could the CSO advise if the incoming MSP is expected to support these as-is? If so, could the CSO confirm that any future strategic requirement to standardise or rebuild these pipelines would be treated as a collaborative project and funded via a separate Statement of Work?	The successful Tenderer will be required to support the in-scope workloads and environment structures as they exist at service commencement. A future requirement to standardise, redesign or rebuild deployment pipelines or environment structures will not automatically form part of the fixed managed-service fee. Where such activity is outside the agreed BAU scope, it may be commissioned through an approved Statement of Work or Contract change, subject to CSO governance, funding and approval.
39	Operations & Service Levels (Appendix 1, Part B, Section 4.5):	Based on the available historic service-desk records, no incidents or service requests logged directly

	To help us accurately right-size our 24/7 support teams, could the CSO share an indicative monthly breakdown of the 141 historic tickets, distinguishing between out-of-hours and standard-hours volume? If this breakdown is not readily available, would the CSO permit tenderers to define their own out-of-hours volume assumptions in the Pricing Schedule, allowing for review via Change Control if actual volumes differ significantly?	by CSO staff during the referenced period were raised outside standard business hours. This does not include monitoring-generated alerts, SOC activity or incidents identified proactively by the MSP outside business hours. From Aug 2025 to Apr 2026 the following tickets were raised: Censushub/Colectica 11 (10 = P3 and 1 = P2), CSO PxStat 64 (6 = P1, 2 = P2, 49 = P3, 6 = P4 and 1 = Lowest), CSO Blaise 12 (12 = P3), Shared Networks 2 (2 = P3), Other CMS General Works 52 (1 =P1, 3 = P2, 47 = P3 and 1 = P4).
40	Operations & Service Levels (Appendix 1, Part B, Section 9.1 & 11.1): To ensure seamless day-to-day operations, could the CSO provide an indicative catalogue of pre-approved "Standard Changes"? In the absence of a catalogue, noting that infrastructure is deployed via CloudFormation, would it be acceptable to assume that modifications to Infrastructure-as-Code will be treated as Normal Changes or project activities rather than routine support?	Modifications to IAC are normal changes and part of routine support if required. Depending on the nature of the change it could be treated as part of project work.
41	Operations & Service Levels (Appendix 1, Part B, Section 6.3): Could the CSO provide guidance on the target resolution times expected for Development and UAT environments? If the CSO intends for these non-production environments to be subject to the same strict 4-hour P1 resolution time as Production, would the CSO be open to funding the architectural upgrades necessary to make these environments Highly Available?	The agreed incident targets will apply according to the priority assigned to the incident, regardless of environment. Incident priority will be determined by impact and urgency. An issue affecting a Development or UAT environment will not automatically be classified as P1 solely because that environment is unavailable. However, a non-production environment may be classified as a high-priority incident where it supports a business-critical activity, release, testing window or major statistical programme. The successful Tenderer must support the current estate as deployed. Any material architectural upgrade required to improve availability, beyond the agreed managed-service scope, may be considered separately through the applicable governance and Statement of Work process.
42	Operations & Service Levels (Appendix 1, Part B, Section 4.2.3 & 4.2.4): To support our capacity planning for major statistical events, could the CSO provide indicative dates and anticipated demand forecasts for the Census 2027 campaign? If this forecasting is not yet available, could the CSO confirm that the required "enhanced service arrangements" for these periods can be scoped and funded collaboratively via separate Statements of Work closer to the time?	Census 2027 and other major statistical programmes will create defined business-critical and peak operational periods. Detailed dates, capacity forecasts and enhanced-support requirements will be communicated through governance and planning as they are confirmed. Routine capacity planning, scaling readiness and operational support for agreed peak periods form part of the managed service. Discrete enhancements, project activity or additional service arrangements outside the routine scope may be separately agreed through a Statement of Work.
43	Commercial & Pricing (Appendix 1, Part B, Section 4.2 & Section 14): Given that several workloads operate on older software versions (Windows Server 2019 and SQL Server 2019), could the CSO confirm if it currently holds Extended Security Update (ESU) agreements? If the CSO does not hold these agreements, could you kindly confirm that tenderers should not include the cost of procuring these ESUs in their fixed recurring price?	Tenderers are not required to include the procurement cost of Extended Security Update agreements within the fixed recurring managed-service fee. Any future requirement for additional licences or Extended Security Update arrangements will be considered separately by CSO through the applicable governance and change-control process. The MSP will remain responsible for lifecycle monitoring, identifying support risks and advising CSO in sufficient time to take appropriate action.
44	Commercial & Pricing (RFT Appendix 2 (Pricing Schedule)): Could the CSO clarify if the single Blended Daily Rate (7.5-hour day) is intended to cover all potential project activities? If it is universal, would the CSO agree that the MSP and the CSO can mutually discuss alternative resourcing models if highly specialised architectural work is requested that cannot be sustainably delivered at the blended rate?	The single Blended Daily Rate is intended to apply to project-based activities falling within the scope of the Services Agreement and the tender documents, including activities agreed through a Statement of Work or formal change control process. Tenderers should therefore price the Blended Daily Rate on the basis that it covers the range of personnel, skills, seniority and expertise required to deliver in-scope project-based activities, including specialist input where required. For any future Statement of Work, the CSO and the Service Provider may agree the scope, deliverables, dependencies, assumptions, timetable, effort and resourcing mix required for the relevant activity. However, any charges based on person-days must be calculated by reference to the tendered Blended Daily Rate. The CSO is not seeking separate role-based rates or alternative daily rates for specialist resources under this Competition.
45	Cybersecurity Operations (Appendix 1, Part B, Section 12.4): To facilitate a highly integrated security response, could the CSO share an indicative RACI mapping the hand-off points between the incoming MSP's SOC and the CSO's existing contracted SOC? If an indicative RACI is unavailable, may we assume for pricing purposes that the MSP's role focuses primarily on initial alerting and containment, with the CSO's SOC leading deep-dive forensics?	The successful Tenderer will retain end-to-end operational responsibility for the AWS SOC and SIEM service, including continuous monitoring, detection, alert triage, investigation, incident response, containment support, evidence preservation, remediation coordination, recovery support, reporting and post-incident review. The CSO will retain governance and oversight of the service and will be kept informed throughout security incidents. The successful Tenderer will provide timely technical advice and recommendations and obtain CSO approval for material actions affecting business services, data, architecture, availability or recovery, except where immediate action is permitted under an agreed incident-response runbook. Tenderers should not assume that their role is limited to initial alerting or containment or that another SOC will assume primary responsibility for incidents affecting the in-scope AWS environment. The successful Tenderer will retain end-to-end operational responsibility and accountability for the SOC service, including where approved subcontractors or specialist third parties are used. The detailed RACI, escalation thresholds, delegated authorities, communication arrangements and incident-response runbooks will be agreed during mobilisation and will remain subject to CSO approval .
46	Transition & Governance (Appendix 1, Part B, Section 17.2): To assist us in building a low-risk Transition-In Plan, could the CSO confirm if the incumbent provider is contractually required to provide knowledge transfer and shadowing support? If such a requirement is not in place, would the CSO act as the primary conduit for knowledge transfer, and kindly allow for flexibility in the transition timeline if incumbent handover delays occur?	The existing service provider will participate in the transition and support agreed knowledge-transfer, shadowing, reverse-shadowing and handover activities. CSO will facilitate access to the in-scope AWS estate, relevant CSO-owned operational tools, documentation, runbooks, reports and available service information, subject to applicable security and access controls. Tenderers should include an effective transition approach that manages documentation gaps and handover risk and does not depend solely on one source of knowledge.
47	Transition & Governance (Appendix 1, Part D & Part B, Section 6.2): Regarding the contingency planning for UK-based Nearshore roles, could the CSO advise on the anticipated notice period it would provide the MSP to relocate roles if the UK loses its data adequacy status? Would the CSO be amenable to granting a minimum implementation window of 90 days to execute this contingency plan without penalty, ensuring a smooth and secure transition?	The CSO is not prescribing a fixed notice period or minimum implementation window for this scenario. As set out in the tender documents, where the United Kingdom ceases to qualify as Nearshore, the MSP will be required to implement its contingency plan within the timeframe specified by the CSO and to ensure that no Restricted Access Role is performed by UK-based personnel from the date specified by the CSO. Any timeframe specified by the CSO would be determined having regard to the applicable legal, regulatory, operational, security and service-continuity circumstances arising at that time.
48	Architecture & Environments (Appendix 1, Part B, Section 4.1 & Section 11.4): To support a structured approach to continuous improvement and technical debt reduction, could the CSO confirm whether a formal AWS Well-Architected Review has been recently conducted for the Landing Zone or the individual workloads? If a recent review has not been completed, would the CSO be agreeable to the incoming MSP undertaking a formal review as a separately scoped project (Statement of Work) early in the contract term to establish an empirical baseline for future optimisation initiatives?	A recent WAR of the LZA has not been completed. A WAR of each workload has been completed as it entered production. Tenderers may recommend a formal landing-zone or workload review as part of their continuous-improvement approach. Any review activity outside the agreed BAU scope may be commissioned separately through an approved Statement of Work, subject to CSO governance, funding and approval.
49	Security & Innovation (Appendix 1, Part B, Section 11.4 & Section 13):	The CSO is open to considering appropriate innovation, automation, GenAI and AIOps proposals,

	To support continuous improvement and operational efficiency, could the CSO confirm its policy regarding the MSP's use of Generative AI (GenAI) and AIOps solutions (e.g., DevOps, Security, or FinOps AI Agents) to assist in service delivery? If the CSO is open to the use of such tooling, could you kindly confirm that provided the AI solutions are hosted within the EEA and comply strictly with the CSO's data protection and confidentiality requirements, tenderers may incorporate these AI-driven efficiencies into their proposed operational model and pricing?	but EEA hosting alone is not sufficient for approval. Any such tooling must receive prior written CSO approval and satisfy security, data-protection, confidentiality, audit, intellectual-property, records-management, access-control and change-governance requirements.
50	For Part 4 of the TRD, are there any word or page limits when answering the questions?	There is no word limit for responses to Part 4 of the TRD. Tenderers should complete the relevant response sections in the TRD using Arial font 11 and single spacing. For clarity, the 3-page limit stated in respect of criterion 2(b) Managed Service Provider Sustainability shall not apply and may be disregarded by Tenderers. Tenderers should ensure that responses are clear, relevant, proportionate and sufficiently detailed to allow the Evaluation Team to assess the Tender in accordance with the Award Criteria set out in the RFT.
51	During the pre-market phase, the authority had mentioned that their current spend within AWS is circa 35,000 Euros a month. may you confirm if this is still the case?	Current spend is in the band of 40,000 - 55,000 Euro per month, we are currently availing of WWPS_SCI (Worldwide Public Sector Science, Cybersecurity, and Innovation). This is an indicative point-in-time range and may vary according to workload demand, usage and changes to the AWS estate. AWS consumption is paid directly by CSO under its AWS commercial arrangement.
52	The authority have mentioned they will retain responsibility for FinOps; cloud financial governance; budgetary control; and the CSO's cloud observability capability shall remain solely with the CSO. With this in mind, what is the expectation for how the potential supplier should work with the CSO when providing a FinOps platform?	A FinOps platform is not a requirement of this tender.
53	What is the expectation for the potential MSP to work with the CSO's internal and external stakeholders mentioned in Appendix 1?	The MSP is expected to work collaboratively and proactively with the CSO's internal teams and relevant external suppliers through the governance, incident, change, security, transition and service-management arrangements set out in the RFT. The MSP will act as the primary operational coordinator for matters within the managed-service scope, while respecting retained CSO decision rights and the contractual responsibilities of other providers. It must maintain clear ownership, escalation, communication and audit trails and must not treat third-party dependency as a reason to relinquish incident or service coordination.
54	With regard to point 8.1, is the authority asking the potential supplier to set the severity definitions by the standards of the potential supplier?	Tenderers should provide their proposed incident severity classification model, including the impact and urgency criteria used to define P1–P4 incidents. The proposed model may be based on the Tenderer's established service-management standards but must meet or exceed the requirements set out in the RFT, including the requirement for 24x7 management of P1 and P2 incidents. The final severity definitions, targets and associated procedures will be agreed with the successful Tenderer during mobilisation and will remain subject to CSO approval.
55	With regard to the mandatory technical requirements outlined in Appendix 1 Part B on the SOC requirements, is the expectation to deploy a 3rd party solution alongside the managed service?	No specific third-party product is mandated. AWS-native services, third-party products or an appropriate combination are acceptable. Refer the Tenderer to revised Section 12 of Appendix 1 Part B v4.1 of Appendix 1 for the detailed requirements.
56	If an MSP cannot provide a SOC for this - can the managed service be a standalone service?	No. The SOC and SIEM capability is a mandatory component of the managed service.
57	Can the Authority provide an inventory of the in-scope existing estate — landing zone(s), AWS accounts/regions, core platform services, in-scope workloads and associated applications, and approximate resource volumes?	The following figures represent an indicative point-in-time snapshot of the AWS estate and may change during the procurement and Contract term. Tenderers should clearly state any material sizing assumptions used in preparing their Tender. Approximate monthly AWS spend (or spend band) €40 - €55,000 monthly. • 7 Workloads AWS Regions - Ireland (eu-west-1) - Frankfurt (eu-central-1) - us-east-1 (billing etc) An indicitive list of AWS Services Breakdown • Accounts — 26 • RDS — 11 (10 active) • DynamoDB — 3 (VDR + Root Account) • EC2 — 63 • Accounts with EC2 — 15 • Accounts with Lambda — 26 • Accounts with SES — 2 • Site to Site VPNS - 2 • Shared Cloud Resources (Accounts) — 9 • Storage Services in use — 8 (EBS, S3, RDS, FSx, EFS, DynamoDB, Glacier, Backup) • Total Storage (GB-Month) — 14,627 GB EC2 in accounts (DEV, PROD, UAT) • Census Recruitment – 11 EC2 • Census Website – 0 • Census Hub – 3 • Blaise – 4 • PXSTAT – 14 • Innovation Hub – 2 • VDR – 25 • Shared Cloud Resources – 4 RDS in accounts (DEV, PROD, UAT) • Census Recruitment – 3 • Census Website – 0 • Census Hub – 1 • Blaise – 0

		• PXSTAT – 3 • Innovation Hub – 2 • VDR – 2 • Shared Cloud Resources – 0 Serverless Services in use (no. of accounts) • Lambda — 26 • SES — 2 • SNS — 26 • SQS — 26 • DynamoDB — 3 (VDR + Root Account) Security Services (no. of accounts) • AWS Shield Advance — 1 (root) • AWS Network Firewall — 1 (shared networks account) • AWS AWS Security Hub — 26 • AWS WAF — 14 (Web ACLs) • Amazon GuardDuty — 26 Governance Services (no. of accounts) • AWS Directory Service — 11 • CloudTrail — 25 • KMS — 26 • CloudWatch — 24 • Config — 26 • Cost Explorer — 1 • CodeBuild — 1 • CodeArtifact — 1 • AWS Backup — 1 Storage Services (no. of accounts, total GB-month) • FSx — 6 accounts — 203.1GB • S3 — 23 accounts — 2556.9 GB • EFS — 5 accounts — 0.8 GB • EBS (Volumes + Snapshots) — 16 accounts — 9591.5 GB • RDS — 10 accounts — 2271.5 GB • AWS Backup (EFS warm storage) — 3 accounts — 2.91 GB • DynamoDB — 3 accounts — 0 GB • Glacier — 5 accounts — 0 GB Networking Services (no. of accounts) • VPC — 14 • Amazon ELB — 12 • Amazon Route 53 — 4 (VDR) • Amazon Kinesis — 3 (VDR + LogArchive) • Amazon Firehose — 1 (Log Archive account) Instance types and count (63 in total) • t3.medium — 14 • r6i.2xlarge — 9 • t3.large — 8 • m5.large — 6 • t3a.xlarge — 3 • t3.2xlarge — 3 • m5.xlarge — 3 • r6i.large — 4 • t2.micro — 2 • t3a.large — 2 • c5.large — 2 • m6a.2xlarge — 2 • t3.xlarge — 2 • t3.small — 1 • r5.xlarge — 1 • m5a.xlarge — 1 RDS Instance Types and count (11 in total) • db.r6i.2xlarge — 5 • db.m6i.xlarge — 3 • db.r5.xlarge — 1 • db.r5.large — 1 • db.r6i.xlarge — 1
58	What are the required service levels (SLAs/KPIs), support hours, and any peak operational periods (e.g. CPI cut-off, Census, statistical-release cycles) the service must sustain?	The service must support 24x7x365 monitoring, alerting and management of P1 and P2 incidents. P3 and P4 incidents will normally be managed during the applicable agreed service hours unless otherwise specified for a workload, peak period or business-critical operational window. Security monitoring and initial security-alert triage must operate on a 24x7x365 basis. The CSO has periods of heightened operational criticality, including Census-related activities, survey-processing deadlines, statistical release cycles and other business-critical periods. The relevant dates and associated service requirements will be communicated and agreed through the service calendar, workload service plans and change-management process. Tenderers must meet or exceed the minimum requirements in the RFT and may propose enhanced service levels.

59	What monitoring, security/SIEM, ITSM/ticketing, backup and DR tooling is currently in use, and is it transferring to the successful tenderer or retained by the Authority?	CSO retains ownership of the in-scope AWS accounts and its cloud observability capability, including Datadog and Pingdom. Relevant AWS-native services, including CloudWatch, CloudTrail, AWS Config, GuardDuty, Security Hub, AWS Backup and other in-scope services, will remain within the CSO AWS estate. The successful Tenderer shall provide the ITSM platform, SOC, SIEM and all other supplier tooling required to deliver the managed service. Incumbent-owned tools, licences, configurations and platforms will not transfer unless expressly stated. The successful Tenderer will be provided with appropriate access to the CSO-owned estate and retained tools during transition.
60	Who is the incumbent provider (if any), what transition support will be made available, and what transition-in window is required before service commencement?	There is an incumbent vendor, appointed in 2024 through an Open Procedure. The current arrangement is being extended to support service continuity during the procurement and transition process. The incumbent will be expected to provide reasonable transition support, including knowledge transfer and the provision of available operational documentation and runbooks. The CSO has not prescribed a fixed transition duration. Tenderers should propose a realistic transition approach and indicative timeframe covering mobilisation, access provisioning, knowledge transfer, documentation validation, shadowing, operational readiness and service handover. The final transition duration, milestones, responsibilities and sequencing will be agreed with the successful Tenderer and the incumbent as part of the Transition-In Plan, subject to CSO approval
61	Please confirm the treatment of United Kingdom resources as Nearshore at the Tender Deadline, and any expectations for the UK-adequacy contingency plan assessed under Criterion 2a.	The definition of Nearshore resources is set out in the RFT and accompanying specification. Refer to clarification #47 for expectations
62	For Restricted Access Roles, are named individuals required at tender stage, or is a resourcing/vetting model with continuity commitments sufficient?	Tenderers are not required to name every individual who may perform a Restricted Access Role at tender stage unless the tender documentation expressly requires named Key Personnel.
63	Does the Tender Response Document structure fully map to Appendix 1 Part B (Detailed Requirements), or is a separate compliance cross-reference to Part B expected?	The Tender Response Document ("TRD") provides the required response structure and maps to Appendix 1 Part B at section/category level rather than on a separate, line-by-line basis. Tenderers should complete each relevant section of the TRD and must ensure that their response addresses all requirements contained within the corresponding section of Appendix 1 Part B, including all Mandatory, Desired and Could requirements, as applicable. Tenderers should use the relevant Appendix 1 Part B section and requirement references within their responses where necessary to demonstrate clearly how the requirements are addressed. However, a separate compliance matrix or standalone cross-reference document is not required. Where any requirement is only partially supported or not supported, the Tenderer must identify the specific requirement concerned and explain any limitation, dependency, assumption, alternative approach or proposed workaround.
64	Please confirm the FinOps boundary: the Authority retains FinOps and pays AWS consumption directly, with the provider giving cost-optimisation recommendations only and no commitment authority.	The CSO retains accountability for FinOps governance and maintains its direct commercial and billing relationship with AWS. The successful Tenderer may implement cost-optimisation measures only following the required CSO review and approval. The successful Tenderer will not have authority to enter into AWS commercial commitments or make binding purchasing decisions on behalf of the CSO unless expressly authorised.
65	What are the Authority's expectations for maintenance windows and change freezes around statistical peak periods (e.g. CPI cut-off, Census processing)?	Maintenance windows will be agreed on a workload-by-workload basis as part of mobilisation and ongoing service planning. The CSO may designate restricted-change or change-freeze periods around Census activities, statistical releases, critical processing deadlines and other peak operational periods. Tenderers must demonstrate how they will plan maintenance and patching around these periods while maintaining security and operational requirements. Emergency changes may be undertaken through the agreed emergency-change process where required to protect security, data integrity or service availability. The applicable service calendar and blackout periods will be maintained and reviewed through the governance and change-management arrangements.
66	For change management, which change classes require Authority approval (CAB), and which may be operated as pre-approved standard changes under an agreed policy?	Typically CAB changes are ones that relate to the broader LZA rather than a specific authorised workload change. E.g. central networking account firewall change, new VPN to be created
67	For disaster recovery, does the Authority invoke DR as a business decision with the provider executing recovery, and what delegation thresholds apply?	The decision to invoke disaster recovery will normally remain a CSO business decision, informed by the successful Tenderer's technical assessment and recommendation. The successful Tenderer will be responsible for executing the approved recovery procedures, coordinating technical activities, maintaining communications and reporting progress. Specific emergency actions may be delegated to the successful Tenderer where these are documented in approved recovery runbooks and are necessary to protect data, security or service continuity
68	Are there transferring personnel under TUPE (SI 131/2003), and if so will anonymised role, tenure and cost data be made available to bidders to price accurately?	TUPE or equivalent arrangements do not apply to this contract.
69	For Criterion 1d, how should committed versus discretionary AWS commercial benefits be represented, and which AWS programmes are in scope for the Authority?	The CSO retains its direct contractual, commercial and billing relationship with AWS. Tenderers should clearly distinguish between: • benefits that are firm and committed as part of the tendered solution; and • discretionary, conditional or potential benefits that may depend on AWS approval, eligibility, future consumption or another third party. No specific AWS partner funding, credit or incentive programme is mandated. Tenderers may identify relevant AWS programmes that could benefit the CSO, but benefits must not be represented as guaranteed unless the Tenderer is in a position to commit to them contractually
70	Is there an indicative pipeline or historical run-rate for project/SoW activity beyond the indicative 200 person-days per annum?	The reference to approximately 200 person-days is an indicative pricing assumption intended to support tender comparison. It is not a guaranteed annual volume, committed pipeline or historical run-rate. Future project and Statement of Work activity will depend on CSO business requirements, funding, governance approvals and the development or onboarding of workloads during the contract term. The CSO does not guarantee any minimum volume or value of project-based activity
71	Please clarify whether the MSP is expected to provide and operate SIEM tooling as part of the service, or whether the MSP is required to consume, investigate and respond to alerts generated by existing CSO-operated SIEM platforms	The MSP must provide, license, implement, operate, maintain and support the SOC and SIEM capability. The MSP is not merely consuming alerts from an existing CSO-operated AWS SIEM. Refer the Tenderer to revised Section 12 of Appendix 1 Part B v4.1 of Appendix 1 for the detailed requirements.
72	Please identify the existing SIEM, security monitoring and threat detection platforms currently operated by or on behalf of the CSO,	The current AWS environment uses relevant AWS-native security and logging services, including AWS CloudTrail, Amazon GuardDuty, AWS Security Hub, AWS Config, Amazon CloudWatch, AWS WAF and AWS Network Firewall.

73	Who is the existing CSO contracted SOC provider	The current AWS environment receives security-monitoring support through the incumbent managed-service arrangements. The identity of the current provider is not material to the preparation of Tenders. The successful Tenderer will be provided with the relevant operational contacts, escalation routes and transition arrangements following Contract award.
74	Please provide indicative monthly volumes for security alerts, security incidents, investigations, escalations and threat-hunting activities -can we assume that Security Incidents are included in the ticket volumes listed in Section 4.5?	A reliable consolidated monthly baseline for security alerts, investigations, escalations, security incidents and threat-hunting activity is not currently available. The service-desk volumes provided elsewhere in the procurement documents should not be interpreted as a complete record of SOC alerts or security activity. Monitoring-generated alerts, investigations and SOC activity are not comprehensively represented in those records. Tenderers should estimate the anticipated SOC and SIEM effort based on the published AWS estate, in-scope workloads, expected log sources and their proposed monitoring and detection model. Tenderers shall clearly state their alert-volume, staffing, tooling, ingestion and pricing assumptions.
75	Please clarify the specific key management responsibilities expected of the MSP (e.g. key creation, rotation, recovery, destruction, certificate management and audit support	The successful Tenderer will be responsible for the agreed operational key-management activities within the in-scope AWS environment, including creation, configuration, rotation, renewal, revocation, recovery, secure deletion, access administration, monitoring and audit support, in accordance with CSO-approved policies, runbooks and change procedures.
76	Please confirm the cryptographic technologies currently deployed (e.g. AWS KMS, ACM, CloudHSM, Secrets Manager and customer-managed encryption keys).	AWS KMS, ACM,Secrets Manager and customer-managed encryption keys, encryption at rest, DB always encrypted, AWS Systems Manager. This is an indicative point-in-time list. A detailed inventory of relevant keys, certificates, secrets and configurations will be made available to the successful Tenderer during transition, subject to applicable security controls.
77	What is the Vulnerability Management tool(s) the MSP is expected to operate?	The successful Tenderer shall provide or coordinate the vulnerability-scanning and vulnerability-management capability required for the in-scope AWS environment. The proposed capability may use AWS-native services, third-party products or an appropriate combination, subject to meeting the RFT and CSO approval. Tenderers shall not assume that an incumbent tool, licence, configuration or service will transfer. All tooling costs required for the proposed managed service shall be included or expressly disclosed in accordance with the Costs Schedule.
	Items 78 to 98 removed - These were duplicated queries inserted into this list for a second time in error	
99	Data Protection Liability Cap (Legal): The Agreement appears to impose unlimited liability in respect of data protection breaches, including under an indemnity. Would the Contracting Authority consider replacing this unlimited liability position with a commercially reasonable liability cap (or super-cap) aligned to market practice for managed cloud services?	The CSO is agreeable to revising the agreement to include an aggregate cap for the breach of these indemnities. Wording to this effect will be included in the revised draft of the agreement to be issued shortly.
100	Scope of CSO Data (Legal): Please confirm whether "CSO Data" includes personal data relating to identified or identifiable individuals and, if so, please provide details of the categories of data subjects and personal data anticipated to be processed under the Services	At present "CSO Data" includes personal data relating to applicants as part of the census recruitment process and employees of the CSO who access and use the AWS platform. The personal data of applicants is standard personal data as would be included in a job application. In the case of employees this is largely names and CSO contract information along with any personal data contained in 'User Data' as defined in the agreement. This may be subject to change over the duration of the agreement as uses of the AWS platform are expanded.
101	Clause 2.13.3 - AWS Incident Management Activities (Legal): Clause 2.13.3 requires the Service Provider to detect, escalate, coordinate and implement remedial measures in relation to incidents attributable to AWS. The provision provides that the Service Provider is not liable for failures attributable to AWS but nevertheless requires the Service Provider to remediate them. As such remediation work may turn out to be considerable, will the customer agree to amend the provision so that additional remediation efforts will be treated as chargeable work and the service provider will be fairly compensated?	The CSO expects standard remediation work would form part of the support services offered by the service provider. If remediation work went beyond typical expectations to the point it was considered an 'Additional Service' this would be addressed using the existing contractual mechanism for this.
102	Section 2.10.6 of the RFT - Inflation adjustment mechanism (Legal): Section 2.10.6 of the RFT provides that prices may be increased or decreased on the first anniversary of the Commencement Date of the Services Agreement subject to the Consumer Price Index. Will the Authority expressly add this as a contract provision in the Agreement and at what stage of the procurement will the amendment be made?	Yes. The inflation adjustment mechanism set out at section 2.10.6 of the RFT will apply to the Services Agreement. Tenderers should prepare their Tenders on the basis that prices may be increased or decreased only in accordance with section 2.10.6 of the RFT. For clarity, the Services Agreement will be completed prior to execution with the successful Tenderer to reflect this mechanism, including in Schedule 2, Fees, and/or Clause 4, Fees, as appropriate. This will give effect to the pricing mechanism already set out in the published tender documents and will not constitute a negotiation or amendment of the tendered pricing mechanism following receipt of Tenders. No separate or alternative inflation adjustment mechanism will apply.
103	Services Agreement acceptance (Legal): Does non-acceptance of the Services Agreement result in disqualification from the procurement?	Yes. Acceptance of the Services Agreement is a requirement of this Competition. Tenderers are required to confirm their acceptance of the terms and conditions of the Services Agreement by signing the Tenderer's Statement. Tenderers may not amend the Services Agreement or qualify their acceptance of it in their Tender. Tenderers may, however, submit queries or requests for clarification in relation to any terms of the Services Agreement through the eTenders messaging facility, in accordance with the process for queries/clarifications set out in the RFT. Where the CSO considers it appropriate to provide clarification, additional context, or any amendment to the tender documents, this will be done through the eTenders messaging facility and made available to all Tenderers. For the avoidance of doubt, no amendments to, qualifications of, or negotiations on the Services Agreement will be permitted following submission of Tenders. A Tender which does not accept the Services Agreement, or which seeks to amend, qualify or take reservation against the terms of the Services Agreement, may be deemed non-compliant and rejected from further consideration.

104	Clause 3.10 - Payment for services performed in case of termination (Legal): Clause 3.10 provides that if the agreement is terminated, the Service Provider is entitled to payment of directly attributable to the proportion of the Services properly completed in accordance with the Agreement, prior to such termination of the Agreement, unless the termination is done pursuant to clause 3.3. This effectively means that if the Authority terminates under clause 3.3, even if the Service Provider has properly completed the Services prior to the termination, it will not be entitled to payment for those Services. Clause 3.3 is broad and lists a number of termination grounds, some of which are no-fault terminations, such as liquidation and Change of Control. We consider this provision unnecessarily onerous to the Service Provider, as it seeks to punish the Service Provider for the termination by not compensating for work properly completed. The principle is that if work is properly completed, it should in all cases be paid for, regardless of termination. Payment for services properly completed should not be made conditional upon whether a termination right is exercised or not. Will the Authority consider removing the link between termination under clause 3.3 and payment of charges for work properly completed?	The CSO can agree to this change, the agreement will be updated to reflect this point.
105	Payment of reasonably committed and property vouched costs (Legal): If the Authority terminates the Agreement pursuant to clause 3.4 (exclusion grounds set out in Article 57 of the Procurement Directive) the Service Provider is entitled to reimbursement for reasonably committed and properly vouched costs. This is fair and should be extended as a principle to termination for convenience under clause 3.5. Will the customer consider an amendment extending the reimbursement for such costs to clause 3.5?	Whilst the CSO appreciates the nature of this request it cannot agree to such an inclusion given the broad range of reasons it may seek to rely on the termination for convenience provision and that any payment would be made using public funds.
106	Clauses 3.8, 4.6 and 4.7 - Objective performance standards (Legal): Clauses 3.8, 4.6 and 4.7 refer to customer dissatisfaction as the trigger for remedial action or the ability to withhold a Retention Amount. Satisfaction is a highly subjective criterion if not accompanied by objective, measurable and pre-agreed acceptance criteria, service levels or specifications. Satisfaction alone may be used arbitrarily and provides a virtually unfettered right for the Authority to reject work and thereby ""enhance or expand" the scope of work, in circumvention of the change control procedure. Will the Authority agree to either remove the reference to satisfaction, or to restrict it by linking it to measurable and objective criteria?	The CSO does not agree to remove the relevant provisions. Clauses 3.8, 4.6 and 4.7 must be read in the context of the Services Agreement as a whole, including the Service Provider's obligation to perform the Services in accordance with the Services Agreement, Schedule 1, Appendix 1 of the RFT, the Service Level Agreement, the applicable specifications, and Good Industry Practice. The CSO does not intend that these provisions will operate as an arbitrary or unfettered right to reject Services or to expand the scope of the Services. Where the CSO requires remedial action or withholds a Retention Amount, the relevant concern must relate to the Services to be provided under the Services Agreement and the applicable contractual requirements, service levels, specifications, standards, deliverables or obligations. For clarity, Clause 4.7 already provides that any Retention Amount must be reasonable and proportionate, and that the CSO must identify the particular Services with which it is dissatisfied together with the reasons for such dissatisfaction. These provisions do not disapply the variation, Statement of Work or change control mechanisms in the Services Agreement. Any change to the nature, scope or timing of the Services, or any requirement for additional services, must be dealt with in accordance with the applicable provisions of the Services Agreement, including the variation and change control provisions.
107	Clause 16.2 - Non-chargeable exit assistance (Legal): Clause 16.2 appears to require exit assistance to be provided without charge following termination under Clause 3.3. The Service Provider considers that Exit Assistance should always be treated as a chargeable activity, regardless of termination. Will the customer agree to amend this provision?	Similarly, the CSO cannot agree to this provision as it would require the payment of additional public funds in circumstances where it has terminated an agreement for cause.
108	Clause 3.11 - One-sided exclusion of loss profits (Legal): Clause 3.11 provides that the Authority is not liable for loss of profit, contracts, goodwill, business opportunity or anticipated savings resulting from termination or otherwise. Will the Authority agree to make this exclusion of the state losses reciprocal?	The CSO can agree to this change, the agreement will be updated to reflect this point.
109	Clause 3.16 - Service Provider liability for replacement service costs (Legal): Clause 3.16 provides that if the Authority terminates under clause 3.3 (iv) (termination for Service Provider liquidation) the Service Provider is liable for the costs for any replacement services provider. Could the customer please explain the rationale for this provision and confirm if it would agree to remove Service Provider liability for replacement services? Compensation for loss can be sought in the ordinary course for breach of contract and monetary damages.	The CSO can agree to the deletion of the portion of clause 3.16 which relates to reimbursement in the event of termination on liquidation. The agreement will be updated to reflect this point.
110	Clause 10 - Suspension rights granted to Authority (Legal): Where Services are suspended by the Contracting Authority under Clause 10, please confirm whether recurring charges will continue to be paid?	Typically, charges are not paid during a suspension scenario as the entire agreement is deemed to be suspended. This is a standard contractual provision which public sector bodies typically include in contracts of this type.
111	Statistics Act 1993 (Legal): Could the Contracting Authority please provide further details regarding the number of personnel anticipated to require appointment as Officers of Statistics under the Act, the circumstances in which criminal or regulatory liabilities could arise, and whether alternative arrangements can be used whereby the Service Provider complies with confidentiality and security requirements without requiring contractor personnel to assume statutory positions or obligations under the Statistics Act 1993?	This inclusion is a statutory requirement of the CSO and no alternative can be agreed to. Every member of service provider personnel who has access to the AWS environment will be considered an Officer of Statistics and will be subject to the relevant conditions. This is as the AWS instance contains statistical data which triggers the obligations under the Statistics Act.
112	Clause 3.5 - Termination for convenience (Legal): Clause 3.5 of the Services Agreement provides that the Authority may terminate the Agreement for convenience on 3 months' notice. Will the Authority agree to add a termination for convenience charge payable to the Service Provider allowing the recovery of reasonably incurred termination-related costs?	The CSO appreciates the nature of this request. However, it is not in a position to agree to such an inclusion given the broad range of reasons it may seek to rely on the termination for convenience provision and that any payment would be made using public funds.
113	4.4 Cost Schedule (2. Project Based Activities): Please confirm whether the blended daily rate for project-based activities is intended to remain the maximum rate for the full contract term before CPI adjustment, or whether the maximum daily rate may also be CPI-adjusted annually.	The tendered Blended Daily Rate for project-based activities shall be the maximum daily rate applicable to such activities, subject only to any CPI adjustment applied in accordance with section 2.10.6 of the RFT and the Services Agreement.

		For clarity, the Blended Daily Rate submitted by the successful Tenderer will apply from the Commencement Date. It may be increased or decreased only on the first anniversary of the Commencement Date and on subsequent anniversaries, and only in accordance with the CPI adjustment mechanism set out in section 2.10.6 of the RFT. Where a CPI adjustment is applied, the adjusted Blended Daily Rate shall become the maximum applicable daily rate for relevant project-based activities from the date of that adjustment, unless and until further adjusted in accordance with the tender documents.
114	4.4 Cost Schedule (Finance): Should Tenderers submit Years 2-5 pricing on a flat-price basis, or should annual CPI increases be reflected within the submitted figures?	Tenderers should not include assumed or forecast CPI increases within the prices submitted for Years 2 to 5. Tenderers should complete the Pricing Schedule by entering their tendered prices in Euro, exclusive of VAT, for each relevant year. Those prices will be used for evaluation as submitted. Any CPI adjustment will apply only after award, and only in accordance with section 2.10.6 of the RFT and the Services Agreement. For clarity, the CSO will not apply any assumed CPI uplift for the purposes of tender evaluation, and Tenderers should not build projected CPI increases into their submitted pricing.
	115 is not used. There is no item corresponding to #115..	
116	Is there currently a SIEM in place? Is so what type?	The current AWS environment uses relevant AWS-native security and logging services, including AWS CloudTrail, Amazon GuardDuty, AWS Security Hub, AWS Config, Amazon CloudWatch, AWS WAF and AWS Network Firewall.
117	Is there a Vulnerability Management Solution in place?	The current AWS environment uses relevant AWS-native security capabilities and incumbent vulnerability-management arrangements. The successful Tenderer shall provide or coordinate the vulnerability-scanning and vulnerability-management capabilities required under revised Section 12 of Appendix 1 Part B v4.1 of Appendix 1, including assessment, prioritisation, remediation tracking and reporting.
118	Is there a SOC service in place?	The current AWS environment receives security-monitoring support through the incumbent managed-service arrangements. The identity of the current provider is not material to the preparation of Tenders. The successful Tenderer will be provided with the relevant operational contacts, escalation routes and transition arrangements following Contract award.
119	How many events are escalated on a monthly basis?	The Contracting Authority does not currently have a reliable consolidated estimate of Events for the in-scope AWS environment. Tenderers should estimate the anticipated ingestion volumes and SOC/SIEM capacity requirements based on the current AWS estate, in-scope workloads, expected log sources and other environment information provided in the procurement documents.
120	What is the Events per second or ingestion volume?	The Contracting Authority does not currently have a reliable consolidated estimate of Events for the in-scope AWS environment. Tenderers should estimate the anticipated ingestion volumes and SOC/SIEM capacity requirements based on the current AWS estate, in-scope workloads, expected log sources and other environment information provided in the procurement documents.
121	What is the total Number and Type of Hosts (Servers) in scope?	The following figures represent an indicative point-in-time snapshot of the AWS estate and may change during the procurement and Contract term. Tenderers should clearly state any material sizing assumptions used in preparing their Tender. Approximate monthly AWS spend (or spend band) €40 - €55,000 monthly. • 7 Workloads AWS Regions - Ireland (eu-west-1) - Frankfurt (eu-central-1) - us-east-1 (billing etc) An indicitive list of AWS Services Breakdown • Accounts — 26 • RDS — 11 (10 active) • DynamoDB — 3 (VDR + Root Account) • EC2 — 63 • Accounts with EC2 — 15 • Accounts with Lambda — 26 • Accounts with SES — 2 • Site to Site VPNS - 2 • Shared Cloud Resources (Accounts) — 9 • Storage Services in use — 8 (EBS, S3, RDS, FSx, EFS, DynamoDB, Glacier, Backup) • Total Storage (GB-Month) — 14,627 GB EC2 in accounts (DEV, PROD, UAT) • Census Recruitment – 11 EC2 • Census Website – 0 • Census Hub – 3 • Blaise – 4 • PXSTAT – 14 • Innovation Hub – 2 • VDR – 25 • Shared Cloud Resources – 4 RDS in accounts (DEV, PROD, UAT) • Census Recruitment – 3 • Census Website – 0 • Census Hub – 1 • Blaise – 0 • PXSTAT – 3 • Innovation Hub – 2 • VDR – 2 • Shared Cloud Resources – 0

		Serverless Services in use (no. of accounts) • Lambda — 26 • SES — 2 • SNS — 26 • SQS — 26 • DynamoDB — 3 (VDR + Root Account) Security Services (no. of accounts) • AWS Shield Advance — 1 (root) • AWS Network Firewall — 1 (shared networks account) • AWS AWS Security Hub — 26 • AWS WAF — 14 (Web ACLs) • Amazon GuardDuty — 26 Governance Services (no. of accounts) • AWS Directory Service — 11 • CloudTrail — 25 • KMS — 26 • CloudWatch — 24 • Config — 26 • Cost Explorer — 1 • CodeBuild — 1 • CodeArtifact — 1 • AWS Backup — 1 Storage Services (no. of accounts, total GB-month) • FSx — 6 accounts — 203.1GB • S3 — 23 accounts — 2556.9 GB • EFS — 5 accounts — 0.8 GB • EBS (Volumes + Snapshots) — 16 accounts — 9591.5 GB • RDS — 10 accounts — 2271.5 GB • AWS Backup (EFS warm storage) — 3 accounts — 2.91 GB • DynamoDB — 3 accounts — 0 GB • Glacier — 5 accounts — 0 GB Networking Services (no. of accounts) • VPC — 14 • Amazon ELB — 12 • Amazon Route 53 — 4 (VDR) • Amazon Kinesis — 3 (VDR + LogArchive) • Amazon Firehose — 1 (Log Archive account) Instance types and count (63 in total) • t3.medium — 14 • r6i.2xlarge — 9 • t3.large — 8 • m5.large — 6 • t3a.xlarge — 3 • t3.2xlarge — 3 • m5.xlarge — 3 • r6i.large — 4 • t2.micro — 2 • t3a.large — 2 • c5.large — 2 • m6a.2xlarge — 2 • t3.xlarge — 2 • t3.small — 1 • r5.xlarge — 1 • m5a.xlarge — 1 RDS Instance Types and count (11 in total) • db.r6i.2xlarge — 5 • db.m6i.xlarge — 3 • db.r5.xlarge — 1 • db.r5.large — 1 • db.r6i.xlarge — 1
122	What is the total Number and Type Network Devices in Scope?	The following figures represent an indicative point-in-time snapshot of the AWS estate and may change during the procurement and Contract term. Tenderers should clearly state any material sizing assumptions used in preparing their Tender. Approximate monthly AWS spend (or spend band) €40 - €55,000 monthly. • 7 Workloads AWS Regions - Ireland (eu-west-1) - Frankfurt (eu-central-1) - us-east-1 (billing etc) An indicative list of AWS Services Breakdown • Accounts — 26 • RDS — 11 (10 active) • DynamoDB — 3 (VDR + Root Account) • EC2 — 63 • Accounts with EC2 — 15 • Accounts with Lambda — 26

• Accounts with SES — 2
• Site to Site VPNS - 2
• Shared Cloud Resources (Accounts) — 9
• Storage Services in use — 8 (EBS, S3, RDS, FSx, EFS, DynamoDB, Glacier, Backup)
• Total Storage (GB-Month) — 14,627 GB

EC2 in accounts (DEV, PROD, UAT)
• Census Recruitment – 11 EC2
• Census Website – 0
• Census Hub – 3
• Blaise – 4
• PXSTAT – 14
• Innovation Hub – 2
• VDR – 25
• Shared Cloud Resources – 4

RDS in accounts (DEV, PROD, UAT)
• Census Recruitment – 3
• Census Website – 0
• Census Hub – 1
• Blaise – 0
• PXSTAT – 3
• Innovation Hub – 2
• VDR – 2
• Shared Cloud Resources – 0

Serverless Services in use (no. of accounts)
• Lambda — 26
• SES — 2
• SNS — 26
• SQS — 26
• DynamoDB — 3 (VDR + Root Account)

Security Services (no. of accounts)
• AWS Shield Advance — 1 (root)
• AWS Network Firewall — 1 (shared networks account)
• AWS AWS Security Hub — 26
• AWS WAF — 14 (Web ACLs)
• Amazon GuardDuty — 26

Governance Services (no. of accounts)
• AWS Directory Service — 11
• CloudTrail — 25
• KMS — 26
• CloudWatch — 24
• Config — 26
• Cost Explorer — 1
• CodeBuild — 1
• CodeArtifact — 1
• AWS Backup — 1

Storage Services (no. of accounts, total GB-month)
• FSx — 6 accounts — 203.1GB
• S3 — 23 accounts — 2556.9 GB
• EFS — 5 accounts — 0.8 GB
• EBS (Volumes + Snapshots) — 16 accounts — 9591.5 GB
• RDS — 10 accounts — 2271.5 GB
• AWS Backup (EFS warm storage) — 3 accounts — 2.91 GB
• DynamoDB — 3 accounts — 0 GB
• Glacier — 5 accounts — 0 GB

Networking Services (no. of accounts)
• VPC — 14
• Amazon ELB — 12
• Amazon Route 53 — 4 (VDR)
• Amazon Kinesis — 3 (VDR + LogArchive)
• Amazon Firehose — 1 (Log Archive account)

Instance types and count (63 in total)
• t3.medium — 14
• r6i.2xlarge — 9
• t3.large — 8
• m5.large — 6
• t3a.xlarge — 3
• t3.2xlarge — 3
• m5.xlarge — 3
• r6i.large — 4
• t2.micro — 2
• t3a.large — 2
• c5.large — 2
• m6a.2xlarge — 2
• t3.xlarge — 2
• t3.small — 1
• r5.xlarge — 1
• m5a.xlarge — 1

		RDS Instance Types and count (11 in total) • db.r6i.2xlarge — 5 • db.m6i.xlarge — 3 • db.r5.xlarge — 1 • db.r5.large — 1 • db.r6i.xlarge — 1
123	What is the total Number of IP addresses in scope for Vulnerability management?	The total number of IP addresses depends on how many appliances are running at anyone time with an IP address. Currently the IP range allocated to the LZA has a total of /15 cidr block in production and /15 cidr block in non-production. The following figures represent an indicative point-in-time snapshot of the AWS estate and may change during the procurement and Contract term. Tenderers should clearly state any material sizing assumptions used in preparing their Tender. Approximate monthly AWS spend (or spend band) €40 - €55,000 monthly. • 7 Workloads AWS Regions - Ireland (eu-west-1) - Frankfurt (eu-central-1) - us-east-1 (billing etc) An indicitive list of AWS Services Breakdown • Accounts — 26 • RDS — 11 (10 active) • DynamoDB — 3 (VDR + Root Account) • EC2 — 63 • Accounts with EC2 — 15 • Accounts with Lambda — 26 • Accounts with SES — 2 • Site to Site VPNS - 2 • Shared Cloud Resources (Accounts) — 9 • Storage Services in use — 8 (EBS, S3, RDS, FSx, EFS, DynamoDB, Glacier, Backup) • Total Storage (GB-Month) — 14,627 GB EC2 in accounts (DEV, PROD, UAT) • Census Recruitment – 11 EC2 • Census Website – 0 • Census Hub – 3 • Blaise – 4 • PXSTAT – 14 • Innovation Hub – 2 • VDR – 25 • Shared Cloud Resources – 4 RDS in accounts (DEV, PROD, UAT) • Census Recruitment – 3 • Census Website – 0 • Census Hub – 1 • Blaise – 0 • PXSTAT – 3 • Innovation Hub – 2 • VDR – 2 • Shared Cloud Resources – 0 Serverless Services in use (no. of accounts) • Lambda — 26 • SES — 2 • SNS — 26 • SQS — 26 • DynamoDB — 3 (VDR + Root Account) Security Services (no. of accounts) • AWS Shield Advance — 1 (root) • AWS Network Firewall — 1 (shared networks account) • AWS AWS Security Hub — 26 • AWS WAF — 14 (Web ACLs) • Amazon GuardDuty — 26 Governance Services (no. of accounts) • AWS Directory Service — 11 • CloudTrail — 25 • KMS — 26 • CloudWatch — 24 • Config — 26 • Cost Explorer — 1 • CodeBuild — 1 • CodeArtifact — 1 • AWS Backup — 1 Storage Services (no. of accounts, total GB-month) • FSx — 6 accounts — 203.1GB • S3 — 23 accounts — 2556.9 GB • EFS — 5 accounts — 0.8 GB

		• EBS (Volumes + Snapshots) — 16 accounts — 9591.5 GB • RDS — 10 accounts — 2271.5 GB • AWS Backup (EFS warm storage) — 3 accounts — 2.91 GB • DynamoDB — 3 accounts — 0 GB • Glacier — 5 accounts — 0 GB Networking Services (no. of accounts) • VPC — 14 • Amazon ELB — 12 • Amazon Route 53 — 4 (VDR) • Amazon Kinesis — 3 (VDR + LogArchive) • Amazon Firehose — 1 (Log Archive account) Instance types and count (63 in total) • t3.medium — 14 • r6i.2xlarge — 9 • t3.large — 8 • m5.large — 6 • t3a.xlarge — 3 • t3.2xlarge — 3 • m5.xlarge — 3 • r6i.large — 4 • t2.micro — 2 • t3a.large — 2 • c5.large — 2 • m6a.2xlarge — 2 • t3.xlarge — 2 • t3.small — 1 • r5.xlarge — 1 • m5a.xlarge — 1 RDS Instance Types and count (11 in total) • db.r6i.2xlarge — 5 • db.m6i.xlarge — 3 • db.r5.xlarge — 1 • db.r5.large — 1 • db.r6i.xlarge — 1
124	Is vulnerability management managed service expected 24/7 or business hours?	Routine vulnerability assessment, remediation planning and reporting will normally be undertaken during the applicable service hours. Critical or actively exploited vulnerabilities must be monitored, escalated and addressed on a 24x7x365 basis where required to protect the environment. Emergency remediation shall follow the agreed incident and emergency-change procedures. Patching and other planned remediation will be scheduled through the agreed maintenance windows and risk-based timescales.
125	How many penetration tests are expected annually	Penetration testing is undertaken by an independent third-party provider appointed by the CSO. The successful Tenderer will not be expected to perform the penetration test unless separately commissioned through an agreed Statement of Work. The successful Tenderer will, however, be required to support the testing process, including planning and scoping discussions, access and technical coordination, provision of relevant information and evidence, review of findings, participation in remediation discussions, implementation of agreed remediation actions within the managed-service scope, tracking of actions to closure and support for any required retesting. The number and timing of penetration tests will be determined by the CSO based on workload risk, material change and assurance requirements. No fixed annual volume is guaranteed
126	What IAM solution is in place or is one required?	The LZA currently uses Entra as its IDP for SSO for CSO staff and AWS IAM for account access management. MSP Staff are currently managed via AWS IAM.
127	What Ticketing system is in place or is one required?	The incumbent provider's ticketing platform will not transfer to the new Contract. The successful Tenderer shall provide, host, license, configure, operate, maintain and support the ITSM platform required to deliver the Service. It must support incident, problem, change, request, knowledge and reporting workflows, together with appropriate integration, access control, auditability, data ownership and export capabilities. All associated costs shall be included in the Tender unless expressly identified and priced in accordance with the Costs Schedule.
128	Is an Incident Response retailer required as part of the service?	The contracting authority understands this refers to an incident response retainer. This is not an requirement under this procurement, if required during the contract this may be commissioned separately through an agree Statement of Work process.
129	What CSO-operated cloud observability and SIEM tooling is in use and required for additional integration?	The CSO retains ownership of its CSO-owned observability tooling. The current environment includes Datadog and Pingdom. The successful Tenderer will be required to integrate with these retained services, consume and respond to applicable alerts, and support the associated operational, security, reporting and audit requirements.
130	To help size the SOC and SIEM, what is the estimated Events per Second (EPS) or Ingestion Volumes (GB) per month	The Contracting Authority does not currently have a reliable consolidated estimate of Events per Second (EPS) or monthly SIEM ingestion volume for the in-scope AWS environment. Tenderers should estimate the anticipated ingestion volumes and SOC/SIEM capacity requirements based on the current AWS estate, in-scope workloads, expected log sources and other environment information provided in the procurement documents.
131	**Scope and existing environment:** Does the new vendor need to migrate a version control repository from the incumbent or the repository is on the CSO side?	No incumbent-owned version-control platform is required to be migrated as a defined transition deliverable. Existing operational documentation, runbooks and knowledge material will be made available to the successful Tenderer during transition where available.
132	**Transition:** Can you please provide an export of the backlog (incidents, service requests, alerts and change backlog) for the last 3 years?	A complete three-year export of incidents, service requests, alerts and change records will not be provided as part of the tender process. The RFT and clarification responses will provide the available summary information considered necessary to support tender preparation, including indicative ticket volumes, workload scope and service characteristics.
133	**Transition:** Will the KB articles be transferred to the new vendor? What Knowledge management tool is currently in use?	The detailed knowledge-transfer arrangements, including the identification and transfer of relevant knowledge articles, runbooks, support documentation and operational procedures, will be agreed as part of the Transition-In Plan. CSO and the existing service provider will support the transition by making available relevant knowledge and documentation relating to the in-scope AWS environment, workloads, operating procedures and known support requirements.

134	**Transition:** Which tools should be migrated from the existing vendor?	No tools are required to be migrated from the existing service provider. The successful Tenderer shall provide, license, configure, operate, maintain and support all supplier-provided tools necessary to deliver the managed service
135	**Transition:** Will the current vendor provide access to the existing toolset for shadowing and reverse-shadowing? Is it agreed with the existing vendor?	The existing service provider will participate in the transition process and will support agreed knowledge-transfer, shadowing, reverse-shadowing and handover activities in accordance with the applicable contractual exit arrangements. The successful Tenderer will be provided with appropriate access to the in-scope AWS estate and all relevant operational tools required to support the transition and subsequent delivery of the managed service. Access will be provided subject to CSO approval, applicable security controls, role-based access, least-privilege principles and the approved Transition-In Plan.
136	**Transition:** Are the transition meetings in the CSO office planned? Was it negotiated with the current vendor?	The Contracting Authority does not require transition meetings to take place at CSO premises. Transition meetings, workshops, knowledge-transfer sessions, governance meetings and service-readiness reviews may be conducted remotely.
137	**Transition:** What switchover windows are allowed to be performed during the transition period?	The Contracting Authority has not prescribed a single fixed switchover window for all transition activities. Switchover arrangements will depend on the workload, business criticality, technical risk, service dependencies and potential user impact.
138	**Scope and existing environment:** Could you please elaborate on how the escalation to CSO's dev team currently works? Is there a joint toolset in use? Is there a global L1 who is responsible for ticket routing?	The current escalation arrangements vary by workload and application support model. Tenderers should not assume that there is a single joint toolset or a single global Level 1 function covering all AWS workloads. Under the new service model, the successful Tenderer shall provide the primary operational service-management function for the managed AWS environment, including initial triage, classification, prioritisation, routing, escalation and coordination of incidents and service requests.
139	**Service Management Framework:** Which ITSM tool is currently used? Where is the current ticketing tool hosted? Which migration options does the new vendor have (if the specific system's name is classified)? What existing integrations with the ticketing system are set?	The incumbent provider's ITSM platform is supplier-owned and will not transfer to the new Contract. The successful Tenderer shall provide, host, license, configure, operate, maintain and support the IT Service Management platform required to deliver the managed service
140	**Service Management Framework:** Is there an existing CMDB, and if so, does the new vendor inherit responsibility for keeping it updated?	The Contracting Authority maintains configuration and asset information for the existing AWS environment.
141	**Scope and existing environment:** Will existing Observability Tool account be transferred to the new vendor or does the new vendor need to bring a new tool/account?	The existing observability account is **CSO-owned** and is expected to remain under CSO ownership. Tenderers should not assume that they are required to provide a replacement observability platform or establish a new account solely for delivery of the managed service
142	CSO maintains its AWS commercial and support relationship directly with AWS. The successful Tenderer will be granted appropriate role-based access to raise, manage, coordinate and escalate AWS Support cases on behalf of CSO, including cases associated with Major Incidents	CSO maintains its AWS commercial and support relationship directly with AWS. The successful Tenderer will be granted appropriate role-based access to raise, manage, coordinate and escalate AWS Support cases on behalf of CSO, including cases associated with Major Incidents. AWS support-subscription charges will remain the responsibility of CSO and should not be included in the managed-service price
143	**Availability, Capacity and Resilience Management:** Are there existing availability targets for the 7 workloads individually, or only aggregate targets, and do these differ by workload criticality (e.g. PxStat's 300-350k daily hits vs. the non-critical Census Hub)?	The Contracting Authority does not currently apply a single aggregate availability target across all seven workloads. Availability, capacity and resilience requirements will be managed at workload level, taking account of business criticality, user impact, service profile, peak periods, technical architecture and upstream or third-party dependencies.
144	**Availability, Capacity and Resilience Management:** Is the single centralized firewall/Transit Gateway/VPN ingress point itself deployed redundantly (multi-AZ, redundant VPN tunnels with BGP failover), and who is accountable for its uptime — MSP or a separate network team?	The centralized firewall is multi AZ as are the TGWs, the current VPNs do not utilise redundant tunnels. The successful Tenderer will be responsible for monitoring, operating, supporting and coordinating incidents affecting the in-scope network services, working with CSO under the agreed RACI.
145	**Security:** Does CSO currently operate a Security Operations Centre (SOC), and if so, what responsibilities remain with the client versus the MSP?	The current AWS environment receives security-monitoring support through the incumbent managed-service arrangements. Under this Contract, the successful Tenderer will retain end-to-end operational responsibility for the SOC and SIEM service supporting the in-scope AWS environment. This includes continuous monitoring, alert triage, investigation, escalation, incident response, evidence preservation and reporting.
146	**Security:** Does the CSO require a dedicated SOC (staff exclusively assigned to the CSO), or is a shared SOC acceptable (analysts serving multiple clients), provided all Onshore/Nearshore location restrictions are met?	A SOC dedicated exclusively to CSO is not required. A shared SOC operating model is acceptable, provided that it is appropriately resourced, meets all 24/7/365 service and security requirements, and complies with the applicable personnel-location, Restricted Access Role, data-access and subcontracting requirements. The SOC and SIEM service supporting the CSO on-premises environment is outside the scope of this procurement. Where a security event, investigation or incident affects, or may affect, both environments, the successful Tenderer shall coordinate with CSO and the relevant on-premises security service provider through the agreed service-management and incident-management procedures. The detailed RACI and coordination arrangements will be agreed during mobilisation. Please refer to revised Section 12 of Appendix 1 Part B v4.1 of Appendix 1 for the detailed requirements
147	**Security:** Would the CSO accept an on-call (standby) model for out-of-hours/night coverage instead of a physically-staffed night shift, provided all SLA response targets and continuous monitoring/alerting are met?	The SOC must be actively operational and appropriately staffed on a 24/7/365 basis. A model relying solely on standby or on-call coverage during overnight periods will not satisfy the requirement for continuous SOC monitoring, alert triage and investigation
148	**Security:** Could you please provide the SLA for Security Incidents and Security Alerts?	The RFT does not prescribe separate response or resolution SLA targets specifically for security alerts or security incidents. The SOC and SIEM service must provide continuous 24x7x365 monitoring, detection and security-alert triage. Where a security alert meets the agreed incident-classification threshold, it shall be recorded and managed as an incident under the agreed general incident-management severity model. P1 and P2 security incidents must be managed on a 24x7x365 basis. Tenderers should provide their proposed: security-alert acknowledgement and triage targets; severity and escalation thresholds; CSO notification targets; incident response and coordination targets; and reporting arrangements. The final operational targets, thresholds and procedures will be agreed with the successful Tenderer during mobilisation, subject to CSO approval.
149	**Security:** To size SOC/monitoring effort, please provide the average number of security alerts generated per month, and their typical distribution — e.g. by severity (P1–P4)	A reliable historical baseline for monthly security-alert volumes and severity distribution is not available. Tenderers should estimate the anticipated alert volumes and associated SOC effort based on the current AWS estate, in-scope workloads and other environment information provided in the procurement documents
150	**Security:** How are responsibilities split between the MSP and the CSO in terms of vulnerability management?	The successful Tenderer shall provide or coordinate vulnerability scanning for the in-scope AWS infrastructure, platform services and workloads; assess and prioritise findings; track remediation; and implement or coordinate patching and configuration remediation within its agreed responsibilities. CSO will retain security governance, risk-acceptance and approval authority. The detailed division of responsibilities will be documented in the agreed RACI during mobilisation.
151	**Security:** Is vulnerability scanning performed today by CSO (or another provider), or is the MSP expected to provide scanning capabilities?	The successful Tenderer is required to provide or coordinate the vulnerability-scanning capability necessary to meet the RFT requirements

152	**Security:** What security tools are currently in use for vulnerability management and security monitoring?	The current AWS environment uses relevant AWS-native services including, as applicable, AWS Security Hub, GuardDuty, CloudTrail, AWS Config, AWS WAF, AWS Network Firewall and CloudWatch. CSO also retains cloud observability tooling including Datadog and Pingdom. These retained services do not replace the Tenderer's obligation to provide the SOC, SIEM, vulnerability-management and associated security tooling required to deliver the Services. A detailed current-state inventory and relevant access information will be provided to the successful Tenderer during transition. Tenderers should not assume that incumbent-owned tools, licences, detection content or configurations will transfer
153	**Security:** Is there a required minimum frequency for scheduled threat-hunting?	The Contracting Authority has not prescribed a fixed minimum frequency for scheduled threat-hunting activities. Tenderers should propose a documented, risk-based threat-hunting methodology and cadence appropriate to the in-scope AWS environment, including scheduled activity and additional hunts triggered by emerging threats, threat intelligence, material environmental changes or security incidents
154	**Security:** Who owns and rotates the KMS Customer Master Keys, and does the MSP get key-administrator or only key-user (encrypt/decrypt) permissions?	The successful Tenderer will perform agreed operational key-management activities, including creation, configuration, rotation, renewal, revocation, recovery, access administration, monitoring and audit support, in accordance with CSO-approved policies, runbooks and change procedures.
155	**Security:** Does the MSP get delegated-admin access in AWS Organizations / Control Tower / Security Hub, or read-only visibility?	The successful Tenderer will be granted the role-based access required to deliver the contracted Services. Access will follow least-privilege, segregation-of-duties, approval, logging and periodic-review requirements.
156	**CSO approval turnaround:** Please confirm expected CSO approval turnaround times for access requests, normal changes, emergency changes, security actions and SoWs, particularly where CSO approval is needed to meet SLA or transition timelines.	The Contracting Authority has not prescribed fixed approval turnaround times for every category of request. Approval times will depend on the nature, risk, complexity and urgency of the request and on the completeness of the information supplied by the successful Tenderer.
157	**Architecture:** Is the ClamAV EKS cluster managed by the MSP end-to-end (cluster upgrades, node patching, CVE remediation etc.)?	Yes. The ClamAV EKS cluster is within the managed-service scope and the successful Tenderer will be responsible for its platform operations, including cluster and node maintenance, upgrades, patching, vulnerability remediation, monitoring, backup and operational support, subject to the agreed RACI.
158	**Expenses treatment:** Please confirm the treatment of travel, on-site attendance, accommodation and subsistence costs, including whether these must be included in the fixed price or billed separately with prior CSO approval. Are any travels to CSO premises expected?	The Services are expected to be delivered primarily remotely, and routine transition or governance meetings are not required to take place at CSO premises. Routine travel and attendance that a Tenderer considers necessary for its delivery model shall be included in the tendered price. Any exceptional on-site attendance requested by CSO must be agreed and approved in advance. No separate reimbursement should be assumed unless expressly approved in accordance with the Contract.
159	**Supplier tooling / third-party tooling costs:** Please confirm whether any supplier-provided tools required to deliver the service, including service desk tooling, monitoring integrations, security tooling, automation tooling or reporting tooling, must be included in the fixed managed service fee unless expressly disclosed in the Costs Schedule. If so, could you provide the indicative number of CSO users for the required toolset?	All supplier-provided tools, licences, integrations and supporting services reasonably necessary to deliver the mandatory managed service shall be included in the tendered fixed managed-service fee unless they are expressly identified and priced separately in the Costs Schedule
160	**Licence and subscription pass-throughs:** Please confirm whether software licence and subscription costs required for the managed service should be treated as CSO-approved pass-throughs, included in the fixed fee, or disclosed as assumptions/exclusions in the Costs Schedule. What are other rules for access and privacy? Who is paying for tokens? Can we use the CSO internal ticketing tool or should we bring our own?	Software licences, subscriptions and other third-party costs required to deliver the Tenderer's proposed managed service shall be included in the fixed managed-service fee unless they are expressly identified and priced separately in the Costs Schedule. AWS consumption incurred directly within CSO-owned AWS accounts will continue to be paid by CSO through its direct AWS arrangements and should not be included as a supplier licence pass-through. Tenderers must nevertheless disclose material AWS consumption associated with their proposed tooling or
161	**Payment milestones for transition-in:** Please confirm whether CSO has a preferred milestone or acceptance basis for invoicing the transition-in price, or whether tenderers should propose this in the Costs Schedule.	"CSO has not set out a preferred milestone or payment schedule for the Transition-In price. Tenderers should set out their proposed milestone basis for invoicing and payment in Sheet 4 – Transition-In Pricing of the Costs Schedule. The proposed payment milestones should be clearly defined, proportionate and aligned with the Tenderer's proposed Transition-In Plan, including the relevant deliverables, transition milestones and service-commencement readiness criteria. Invoicing should be linked to the completion of the relevant milestone and its acceptance by the CSO. Payment of valid invoices will be made in accordance with the payment provisions of the Services Agreement."
162	**Treatment of material workload growth:** Please confirm how material growth in the existing estate, for example additional AWS accounts, workloads, environments, support coverage or ticket volumes, will be treated where it goes beyond the assumptions in the tendered fixed fee.	Reasonable organic growth in the current in-scope estate, including ordinary variation in resource, ticket and alert volumes, shall be accommodated within the tendered fixed managed-service fee. Tenderers shall state the material baseline and capacity assumptions used in preparing their Tender. Significant expansion of scope, such as onboarding substantial new workloads, environments or support obligations, may be managed through an approved Statement of Work.
163	**Service credits / penalties:** Please confirm whether SLA service credits, rebates, liquidated damages or other financial remedies will apply for SLA failure.	The Contracting Authority confirms that the RFT does not provide for an automatic regime of SLA service credits, rebates or liquidated damages in respect of SLA failure. The agreed Service Levels will form part of the contractual performance requirements and will be monitored through the service-management and governance arrangements. Where performance falls below the agreed Service Levels, the successful Tenderer may be required to investigate the cause, implement corrective actions, provide a Service Improvement Plan and report progress through the agreed governance process
164	**(Liability and indemnities)** Clause 11.1 – uncapped liability heads. Clause 11.1 excludes liability under Clauses 6, 7.9, 13 and 16.8 from the 1.5× Fees cap, leaving these unlimited. Given the operational monitoring and support nature of the Services, would the CSO consider applying an aggregate cap to these excepted heads? If not, please confirm the CSO's expectation that tenderers price for unlimited exposure on these heads.	The CSO is agreeable to revising the agreement to include an aggregate cap for the breach of these indemnities. Wording to this effect will be included in the revised draft of the agreement to be issued shortly.
165	**(Liability and indemnities)** Clause 11.3 We note that 3.11 excludes certain heads of loss on behalf of the CSO, whereas Clause 11.3 excludes liability for "indirect or consequential losses." It is standard practice in the Irish market for limitation-of-liability clauses to excluded heads of loss (loss of profit, revenue, anticipated savings, goodwill, business/opportunity) Please confirm the Contracting Authority is agreeable to amending Clause 11.3 to make the exclusion of these heads of loss mutual for both parties.	The CSO can agree to this change, the agreement will be updated to reflect this point.

166	**(Liability and indemnities)** Clauses 7.9 / 13.7 / 6.5 / 16.8 – scope of indemnities. These indemnities are one-way and unqualified. For the IP indemnity at Clause 7.9, would the CSO clarify this to provide that this is due to the Service Providers' fault (and that we are not responsible for any third party claims from use of a third party product provided by AWS or any other third party) subject to 7.10 and accept customary carve-outs (CSO-supplied data/materials/instructions, use of Deliverables other than as authorised, and infringements arising only from combination with items not supplied by the Service Provider)? Would the CSO also confirm that liability under these indemnities is intended to arise only to the extent of the Service Provider's fault and where breach of legislation is listed that such breaches are limited to those arising during the course of the services?	The CSO appreciates this query but will not be making changes to the wording of the indemnities contained in the agreement.
167	**(Standard of care and scope)** Clauses 2.5 / 2.7 – standard of care. Clause 2.5 refers to "reasonable care, skill and ability," while Clause 2.7 imports "Good Industry Practice" benchmarked against a "leading service provider." Please confirm which standard governs in the event of inconsistency, and whether the CSO would consider a single "reasonably skilled and experienced provider" benchmark.	Clause 2.5 to be revised to refer to Good Industry Practice to avoid any ambiguity on this point.
168	**(Standard of care and scope)** Advisory activities. Certain Services (e.g. reviewing release strategy, assessing and advising on incidents and performance) are advisory, with strategic and architectural authority retained by the CSO under Clause 2.12.4. Please confirm that the Service Provider is not liable for CSO decisions taken on foot of such recommendations.	This is confirmed, the service provider is not intended to be responsible for the CSO's decisions in connection with the items listed in clause 2.12.4 but will be responsible for its own actions taken in carrying out these decisions as would be expected.
169	**(Termination and payment)** Clauses 3.5 / 3.6 – termination symmetry. The CSO may terminate for convenience on three months' notice (Clause 3.5), whereas the Service Provider may terminate only for CSO material breach (Clause 3.6). Would the CSO consider adding a Service Provider right to terminate for persistent non-payment of undisputed sums?	Non-payment of undisputed sums on a consistent basis would be a material breach of clause 4 of the agreement and would be captured by clause 3.6. The CSO considers that a standalone termination right is therefore not required.
170	**(Termination and payment)** Clause 3.3 – change of control. Clause 3.3(v) permits termination on a change of control. Would the CSO confirm that a bona fide intra-group reorganisation that does not materially affect the Service Provider's ability to perform is not intended to trigger this right?	A bona fide intra-group reorganisation would typically not 'materially affect the Service Provider's ability to carry out the Agreement' as is required in clause 3.3(v) and is therefore not intended to be captured by this clause.
171	**(Termination and payment)** Clauses 4.7 / 4.8 – withholding. Clause 4.7 allows the CSO to withhold a "Retention Amount" on dissatisfaction while Clause 4.8 requires continued performance during disputes. Please confirm that any withholding will be limited to the reasonable value of the affected Services and supported by written, itemised reasons and can the CSO consider a time limit for retention and a maximum amount which can be withheld (e.g. no more than 5% of the charges relating to the affected services).	The retention is already specified as being for a 'reasonable and proportionate sum' and clause 4.7 requires the CSO to 'identify the particular services with which it is dissatisfied together with the reasons for dissatisfaction'. The CSO considers that, aside from a time limit for retention, the points raised are largely already addressed in the clause, albeit using different language.
172	**(IP) 1. Clauses 7.1 / 7.4** – Background IP. Please confirm that the Service Provider's pre-existing and independently developed monitoring tools, scripts, runbooks and methodologies remain Background Intellectual Property and are not captured by the assignment of Deliverables Intellectual Property in Clause 7.4 (consistent with Clause 16.3).	This is correct, the definition of 'Background Intellectual Property' addresses this point in specifying that this includes IP *'which are or have been developed independently of this Agreement, the Services and Deliverables'*. If IP was developed prior to or independently to the agreement it would be considered Background IP.
173	**(AWS Terms)** We note that Clause 2.2 provides that, in the event of conflict between the Agreement and the AWS Terms, the Agreement shall prevail, but acknowledges that certain AWS Terms are imposed on CSO by AWS and may not be capable of amendment, and requires the Service Provider to comply with the AWS Terms and to notify CSO where compliance would conflict with the Agreement. The AWS Terms are contracted between the CSO and AWS directly. The Service Provider is not a party to those terms and is therefore not privy to their content, and has no visibility of, or control over, their scope or any subsequent amendment by AWS. As drafted, Clause 2.2 could expose the Service Provider to obligations (and a corresponding duty to identify conflicts and act consistently) by reference to a document to which it is not party and which it may never have seen. It is not reasonable, and not standard practice in the Irish market, for a supplier to be bound by, or to warrant compliance with, terms agreed between the Contracting Authority and a third party that are outside the supplier's knowledge and control. Please confirm the Contracting Authority is agreeable to amending Clause 2.2 to (a) limit the Service Provider's obligations to those AWS Terms that have been disclosed to the Service Provider in writing prior to the relevant obligation arising, and (b) confirm that the Service Provider shall not be in breach of, or liable under, this Agreement as a result of any AWS Term (or amendment to any AWS Term) that has not been so disclosed	The CSO intends to share the relevant portions of the AWS Terms with the chosen provider following contract award to ensure these can be complied with. For context, the AWS Terms are (subject to minor amendments) the AWS standard enterprise terms for a solution of this type.
174	**(Audit) Clause 5.7** permits the CSO to conduct audits "at any time" on fourteen (14) days' notice (and with no notice in an emergency), but places no limit on the number or frequency of audits and does not define which documents and records fall within scope. Read with the Service Provider's broad disclosure obligations under Clauses 5.4–5.6, this could expose the Service Provider to open-ended and disproportionate audit activity, and to requests for records unconnected with the Services (including the Service Provider's proprietary or commercially sensitive materials and other clients' data). Accordingly, the Service Provider requests that the CSO confirm whether it would accept the following clarifications to Clause 5.7: 1) limit of audits to on per year save where required by law or a regulator, 2) the right of audit extends only to those documents, records, systems and data that relate to the Service Provider's performance of the Services and its obligations under this Agreement, 3) audits will be conducted during normal business hours, in a manner that minimises disruption to the Service Provider's business and 4) Please confirm which party bears the Service Provider's reasonable costs of supporting audits, and in particular that the Service Provider's cooperation time will be chargeable where an audit is not prompted by a Service Provider default	Items 1-3 listed in the query are acceptable and the agreement will be updated to reflect these points. In relation to item 4, Service Provider co-operation with audits is considered to be a standard part of contract management and, accordingly, co-operation time will not be chargeable.

175	**(Insurance)** Noting CSO's interest / indemnity to principals (12.3).Our insurers can note the customer's interest / provide indemnity-to-principal status only under the public/general liability (and motor) policies. Would the CSO confirm this requirement applies to the public liability policy only, and not to the professional indemnity, employer's liability or cyber policies?	The CSO appreciates this query but is not in a position to accept this proposed change to the wording of clause 12.3.
176	**(Insurance)** Evidence of cover (12.7). Please confirm certificates of insurance (rather than copies of the underlying policies) are acceptable evidence of cover.	This amendment is accepted and the agreement will be updated to reflect this point.
177	**(Data Protection) Clause 13.3.9** goes beyond what is required of a data processor under Irish and EU data protection law, in two respects, and the Service Provider requests the following clarifications/amendments: 1. Notification timing. Under Article 33(2) GDPR, a processor's obligation is to notify the controller of a personal data breach "without undue delay" after becoming aware of it. The fixed 24-hour deadline in Clause 13.3.9 is a stricter, absolute standard that does not align with the statutory obligation and may be impractical where a breach is still being triaged. Would the CSO confirm that "without undue delay" (consistent with Article 33(2) GDPR) is acceptable in place of the fixed 24-hour period? 2. Restoration of Personal Data. As drafted, the obligation to restore Personal Data "at its own expense" is unqualified — it applies regardless of cause, including loss or corruption arising from acts of the CSO, AWS, or other third parties outside the Service Provider's control. Would the CSO confirm that the Service Provider's restoration obligation is limited to circumstances where the loss, destruction, damage or corruption was caused by the Service Provider's breach of this Agreement or its negligence, and that restoration is to be effected from the most recent available back-up?	**Breach notification:** The CSO appreciates that the 24-hour notification period goes beyond strict regulatory timeframes. However, EDPB guidance on this area suggests the inclusion of a specific time period in Article 28 data processing agreements. Given the CSO's role as a statutory body, it requires contractual certainty as to when it will be notified of a breach and is therefore not in a position to revise this wording. **Restoration of personal data:** The CSO is not in a position to accept changes to its standard data protection processing provisions. The restoration of data will be addressed more generally in the disaster recovery plan.
178	**(Data Protection) Clause 13.6** gives effect to the CSO's audit right under Article 28(3)(h) GDPR but is broader than necessary. Would the CSO confirm that, before conducting an on-site inspection, it will first have regard to documentary evidence of compliance (such as certifications, audit reports and responses to written questionnaires); that the inspection right is limited to facilities, documents and data relating to the Processing of CSO's Personal Data under this Agreement (and not other clients' data or the Service Provider's wider systems); that audits will be no more than once in any 12-month period (save where a supervisory authority requires it or the CSO reasonably suspects a Personal Data Breach); that they will be conducted during normal business hours with minimal disruption; and that any CSO representatives will be bound by confidentiality and will not be competitors of the Service Provider?	As noted in the preceding query, the CSO is not in a position to accept changes to its standard data protection processing provisions.
	179 is not used. There is no item corresponding to #179.	
	"Can the Authority provide an inventory of the in-scope existing estate: — landing zone(s) — AWS accounts/regions — core platform services — in-scope and out-of-scope workloads and associated applications — approximate resource volumes & quantities (criteria pertains to single site. replicated. HA, DR etc.) — VMs (OS, vCPU, RAM, disk type and size(s)) — Storage (sizes and performance tiers) — NICs"	The following figures represent an indicative point-in-time snapshot of the AWS estate and may change during the procurement and Contract term. Tenderers should clearly state any material sizing assumptions used in preparing their Tender. Approximate monthly AWS spend (or spend band) €40 - €55,000 monthly. • 7 Workloads • OS Breakdown, approximately 90% windows, 10% linux AWS Regions - Ireland (eu-west-1) - Frankfurt (eu-central-1) - us-east-1 (billing etc) An indicitive list of AWS Services Breakdown • Accounts — 26 • RDS — 11 (10 active) • DynamoDB — 3 (VDR + Root Account) • EC2 — 63 • Accounts with EC2 — 15 • Accounts with Lambda — 26 • Accounts with SES — 2 • Site to Site VPNS - 2 • Shared Cloud Resources (Accounts) — 9 • Storage Services in use — 8 (EBS, S3, RDS, FSx, EFS, DynamoDB, Glacier, Backup) • Total Storage (GB-Month) — 14,627 GB EC2 in accounts (DEV, PROD, UAT) • Census Recruitment – 11 EC2 • Census Website – 0 • Census Hub – 3 • Blaise – 4 • PXSTAT – 14 • Innovation Hub – 2 • VDR – 25 • Shared Cloud Resources – 4 RDS in accounts (DEV, PROD, UAT) • Census Recruitment – 3 • Census Website – 0 • Census Hub – 1 • Blaise – 0 • PXSTAT – 3 • Innovation Hub – 2 • VDR – 2 • Shared Cloud Resources – 0 Serverless Services in use (no. of accounts)

180		• Lambda — 26 • SES — 2 • SNS — 26 • SQS — 26 • DynamoDB — 3 (VDR + Root Account) Security Services (no. of accounts) • AWS Shield Advance — 1 (root) • AWS Network Firewall — 1 (shared networks account) • AWS AWS Security Hub — 26 • AWS WAF — 14 (Web ACLs) • Amazon GuardDuty — 26 Governance Services (no. of accounts) • AWS Directory Service — 11 • CloudTrail — 25 • KMS — 26 • CloudWatch — 24 • Config — 26 • Cost Explorer — 1 • CodeBuild — 1 • CodeArtifact — 1 • AWS Backup — 1 Storage Services (no. of accounts, total GB-month) • FSx — 6 accounts — 203.1GB • S3 — 23 accounts — 2556.9 GB • EFS — 5 accounts — 0.8 GB • EBS (Volumes + Snapshots) — 16 accounts — 9591.5 GB • RDS — 10 accounts — 2271.5 GB • AWS Backup (EFS warm storage) — 3 accounts — 2.91 GB • DynamoDB — 3 accounts — 0 GB • Glacier — 5 accounts — 0 GB Networking Services (no. of accounts) • VPC — 14 • Amazon ELB — 12 • Amazon Route 53 — 4 (VDR) • Amazon Kinesis — 3 (VDR + LogArchive) • Amazon Firehose — 1 (Log Archive account) Instance types and count (63 in total) • t3.medium — 14 • r6i.2xlarge — 9 • t3.large — 8 • m5.large — 6 • t3a.xlarge — 3 • t3.2xlarge — 3 • m5.xlarge — 3 • r6i.large — 4 • t2.micro — 2 • t3a.large — 2 • c5.large — 2 • m6a.2xlarge — 2 • t3.xlarge — 2 • t3.small — 1 • r5.xlarge — 1 • m5a.xlarge — 1 RDS Instance Types and count (11 in total) • db.r6i.2xlarge — 5 • db.m6i.xlarge — 3 • db.r5.xlarge — 1 • db.r5.large — 1 • db.r6i.xlarge — 1
181	Are there any 3rd party applications and/or services (i.e. not found, procured or connected to the AWS marketplace) in scope ?	Yes, the in-scope AWS environments includes third-party applications, products and services. The successful tenderer will not be responsible for managing, administering or providing functional support for those third party applications systems unless expressly stated in the RFT or subsequently agreed through a SOW
182	We are just wondering if you received our clarification queries that we submitted on the 10th of July please? Just some of our tender responses hinge on the answers to those clarifications. With this in mind, would it be possible to request an extension to the response deadline to the 7th of August at 5pm, if possible please?	All clarifications received as of COB on July 20 2026 are listed in this document. The clarification and tender submission deadlines have been extended. Please refer to the separate clarification and updated eTenders notice for details.
183	Can CSO provide a high-level view of current AWS consumption, including monthly AWS spend.	Please refer to clarificaiton 180

184	Can CSO provide available historical and current operational volumetrics relevant to the managed service, including: a. the average monthly volume of operational alerts generated from Datadog, CloudWatch and other monitoring platforms; b. the number of active Datadog monitors, dashboards and synthetic monitoring checks; c. the average monthly volume of security alerts and the approximate annual number of security incidents requiring investigation and escalation; d. historical ticket volumes by application or service, including ticket priority and the percentage requiring out-of-hours support; e. historical major incident volumes and any known recurring service or operational issues; and f. indicative number of operational users, privileged users and application support users across the managed environment?	Available historical service-desk volumes are provided in Clarification 6. Available security and vulnerability-management information is provided in Clarifications 74, 119, 120, 123, 149, 150 and 151. A reliable consolidated historic baseline for Datadog/CloudWatch alert volumes, active monitor/dashboard/synthetic-check counts, major-incident volumes or the requested user categories is not currently available for tender purposes. Tenderers should use the published estate information and clearly state any material sizing assumptions
185	Can CSO provide the expected Census 2027 peak user volumes, transaction volumes and any specific enhanced support expectations during census-related operational periods?	Fixed durations for enhanced support periods have not yet been defined. Enhanced support arrangements will be planned in advance of Census 2027 and other major business events and may include increased monitoring, operational readiness reviews, restricted change windows, enhanced escalation, senior technical availability and more frequent reporting and will be defined and agreed through out a SOW.
186	Can CSO provide indicative volumes for Infrastructure-as-Code repositories, CloudFormation templates, automation artefacts, operational runbooks and support documentation currently in use?	A consolidated count of Infrastructure-as-Code repositories, Cloud Formation templates, automation artefacts, runbooks and support documentation is not currently available for tender purposes. Relevant repositories, automation artefacts, documentation and runbooks required to operate the in-scope environment will be made available during transition, where available.
187	Can CSO provide details of current vulnerability volumes by severity, including average monthly high and critical vulnerability findings and remediation targets?	A reliable consolidated monthly baseline of vulnerability findings by severity is not currently available. Please refer to Clarifications 150 and 151 and Replacement Section 12 of Appendix 1 for the vulnerability-management responsibilities and operating requirements.
188	Can CSO confirm the planned date on which the successful Tenderer will assume full operational responsibility?	The successful Tenderer will assume full operational responsibility following completion and CSO acceptance of the agreed Transition-In activities and operational-readiness criteria.
189	What level of involvement and knowledge transfer will be provided by the incumbent Managed Service Provider during transition, including access to documentation, runbooks, repositories, operational procedures and shadowing and reverse-shadowing activities?	Please refer to Clarifications 46 and 60 regarding incumbent participation, transition, knowledge transfer, shadowing and reverse-shadowing.
190	Can CSO provide workload-specific Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs) and availability targets for each in-scope workload where these differ from the general service levels defined within the RFT?	Workloads have differing business criticality, architectures and recovery requirements. A complete workload-specific schedule of RTOs, RPOs and availability targets is not being provided for tender purposes. Relevant existing recovery and availability requirements will be provided during transition and validated with application owners
191	Can CSO provide historical annual volumes for Standard, Normal and Emergency Changes together with typical approval lead times, maintenance windows and any planned change freeze periods?	Approval lead times will depend on the risk, urgency, completeness and impact of the proposed change. Maintenance windows and change-freeze periods will be agreed according to workload requirements and major operational events. Please also refer to Clarifications 40, 66 and 156.
192	Can CSO clarify the expected duration and scope of enhanced operational support periods associated with Census 2027 and other major business events?	Fixed durations for enhanced support periods have not yet been defined. Enhanced support arrangements will be planned in advance of Census 2027 and other major business events and may include increased monitoring, operational readiness reviews, restricted change windows, enhanced escalation, senior technical availability and more frequent reporting. The detailed scope and duration will be agreed in advance and, where the requirement falls outside the contracted managed-service scope, may be commissioned through an approved Statement of Work.
193	Can CSO provide the number of active VDR research projects, researchers and VDI environments currently supported?	The VDR service is currently being built and is not yet in live operational use. There are therefore no current VDR research projects, active VDR researchers or live VDR environments to report. The VDR service is intended to replace the existing ROSA service. For indicative context only, the current ROSA service supports approximately 340 active researchers across 176 active projects. These ROSA figures are provided as an indication of the existing research-service scale and should not be interpreted as guaranteed VDR volumes.
194	Can CSO provide the approximate annual number of new research projects or VDR onboarding requests?	The VDR service is not yet live and therefore does not currently have an established annual onboarding volume. For indicative context, the existing ROSA service approved 97 new projects during 2025 and 47 new projects to date in 2026. These figures are provided as an indication of historic demand for the service that VDR will replace and should not be interpreted as a guaranteed future VDR onboarding volume.
195	Can CSO provide historical annual effort consumption for project-based activities and Statements of Work over the previous three years?	Historically, Statements of Work were generally raised for the onboarding and implementation of individual AWS accounts and associated workloads on the AWS platform. The current AWS accounts and estate information provided elsewhere in the clarification responses therefore gives an indicative view of the scale of this activity. A consolidated historic breakdown of person-days or expenditure under Statements of Work over the previous three years is not being provided.
196	Does CSO have any currently identified future workloads expected to be onboarded into the managed service during the initial contract term?	No complete or committed roadmap of platform upgrades, application migrations or major operational changes is being provided. CSO expects the AWS estate to evolve during the Contract term, including the onboarding or modification of workloads associated with major statistical programmes and business requirements.
197	Can CSO clarify which security services remain with CSO or third-party providers and which are expected to transfer to the MSP, particularly regarding SOC operations, SIEM monitoring and incident response?	The successful Tenderer will retain end-to-end operational responsibility for the SOC and SIEM service supporting the in-scope AWS environment. CSO will retain security governance, oversight, risk acceptance and material approval authority. The on-premises SOC/SIEM service remains outside scope, with operational coordination required where events or incidents affect both environments. Please refer to Replacement Section 12 of Appendix 1.
198	Can CSO confirm whether any workload-specific availability, response or recovery objectives apply beyond the service levels defined within the RFT?	Please refer to clarificaiton 37, 41 and 58
199	Can CSO provide a high-level responsibility matrix identifying the respective responsibilities of the CSO, the Managed Service Provider, application support teams, AWS and any other third-party service providers?	Please refer to clarificaiton 32 & 181

200	Where incidents originate within application code or third-party managed services, is the successful Tenderer expected to retain end-to-end incident ownership and coordination until full service restoration?	The successful Tenderer will retain incident coordination and service-management ownership until service restoration, including triage, escalation, infrastructure investigation, stakeholder coordination and communications. Responsibility for resolving defects within application code, third-party products or supplier-managed applications will remain with the relevant application owner or third-party supplier. The MSP will not be responsible for application-code remediation unless expressly included in scope.
201	Can CSO clarify which application support activities are expected to be delivered by the Managed Service Provider and which will remain the responsibility of CSO application teams or other third-party suppliers?	Please refer to claificaiton No 181
202	Can CSO provide the outcomes of the most recent Disaster Recovery, backup restoration and Business Continuity tests, including any outstanding actions relevant to the managed service?	Detailed outcomes of previous Disaster Recovery, backup-restore and Business Continuity tests will not be provided as part of the tender process. Relevant current test records, recovery documentation, known actions and remediation items required to operate the in-scope services will be made available to the successful Tenderer during transition, subject to applicable security controls.
203	Which IT Service Management (ITSM) platform is currently used by CSO, and is the successful Tenderer expected to use the existing platform, integrate with it, or provide its own ITSM tooling?	The incumbent provider's ITSM platform is supplier-owned and will not transfer. The successful Tenderer shall provide, host, license, configure, operate, maintain and support the ITSM platform required to deliver the Services.
204	Can CSO provide details of the existing integrations between AWS, Datadog, CloudWatch, the IT Service Management (ITSM) platform, Security Information and Event Management (SIEM) tooling, and any other operational platforms relevant to the managed service?	The AWS environment currently uses AWS-native monitoring and logging services, including CloudWatch and CloudTrail, together with CSO-owned observability tooling including Datadog and Pingdom. The successful Tenderer will provide its own ITSM platform and the SOC/SIEM capability required under Replacement Section 12. Tenderers should propose the integrations necessary to deliver an effective operating model.
205	Does CSO currently maintain a Configuration Management Database (CMDB) or equivalent configuration repository, and if so, what is its current level of completeness and accuracy?	Please refer to claificaiton No 140
206	Are there any significant platform upgrades, technology refreshes, application migrations or other major operational changes currently anticipated during the initial contract term?	No complete or committed roadmap of platform upgrades, application migrations or major operational changes is being provided. CSO expects the AWS estate to evolve during the Contract term, including the onboarding or modification of workloads associated with major statistical programmes and business requirements.
207	We note the Authority's response under item 106 in relation to the question whether clauses 3.8, 4.6 and 4.7 (customer dissatisfaction as a trigger for remedial action) will not be removed from the agreement. The Authority has stated that the intent behind the clause is for the measurement of dissatisfaction to be assessed against the agreed service levels, specifications, standards, deliverables or obligations and not arbitrarily. If that's the intent, will the Authority agree to expressly add the reference to the agreed service levels, specifications, standards, deliverables or obligations to the clause so as to ensure complete legal certainty and avoid any ambiguity in interpretation?	Whilst the CSO appreciates this request for amendment it is not in a position to agree to making these changes to the clause wording. Remediation of defective works is a reasonable inclusion and as noted in the previous response any remediation or retention exists only within the current contractual framework and is not something the CSO intends to use arbitrarily.
208	In order to be able to hone our response to the single blended rate question in the Price Sheet, we would appreciate some sight of what, historically demand has been. This single number looks to be 35% of the scoring with a ratcheting mechanism favouring the lowest price. A view of past demand and/or expected demand, will help us get to our most competitive pricing.	Please refer to Clarification 195. CSO does not have a consolidated historic person-day breakdown. The current AWS estate and account information provided elsewhere in the clarification responses provides an indicative view of historic project activity. Future Statement of Work demand is not guaranteed and will depend on business requirements during the Contract term
209	Please confirm whether the ClamAV EKS platform consists of a single EKS cluster or multiple clusters, and whether any additional Kubernetes workloads besides ClamAV are currently within scope.	The following figures represent an indicative point-in-time snapshot of the AWS estate and may change during the procurement and Contract term. Tenderers should clearly state any material sizing assumptions used in preparing their Tender. - All EKS managed via fargate - 1 Accounts - in production - 4 Accounts - non production - 1 cluster per account. - Total 5 Clusters - 0 node groups, - 0 ec2 worker nodes, - 18 namespaces - 0 deployed pods
210	Please provide the current EKS inventory including the number of clusters, node groups, EC2 worker nodes, namespaces and deployed workloads/pods.	The following figures represent an indicative point-in-time snapshot of the AWS estate and may change during the procurement and Contract term. Tenderers should clearly state any material sizing assumptions used in preparing their Tender. - All EKS managed via fargate - 1 Accounts - in production - 4 Accounts - non production - 1 cluster per account. - Total 5 Clusters - 0 node groups, - 0 ec2 worker nodes, - 18 namespaces - 0 deployed pods
211	Please confirm the availability, backup, DR and recovery requirements applicable to the ClamAV EKS environment, including any multi-AZ deployment requirements and target recovery objectives.	Workloads have differing business criticality, architectures and recovery requirements. A complete workload-specific schedule of RTOs, RPOs and availability targets is not being provided for tender purposes. Relevant existing recovery and availability requirements will be provided during transition and validated with application owners
212	Please provide the typical frequency of Kubernetes upgrades, node updates, security patching and maintenance activities currently performed on the ClamAV EKS environment.	Maintenance windows for Kubernetes upgrades, node updates, and security patching and maintenance on the ClamAV EKS environment will be agreed on a workload-by-workload basis as part of mobilisation and ongoing service planning.