

Appendix 1: Requirements and Specifications

0 Background

This section provides background to this Call for Tender (CfT) and summarises the key goals and requirements that Autism Spectrum Information, Advice and Meeting Point CLG (“AsIAM”) is seeking from a Managed Service Provider (MSP) through this tender.

0.1 Profile of AsIAM

AsIAM is Ireland’s National Autism Charity, and an Autistic-led organisation operating under Section 39 of the Health Act. We are dedicated to removing the invisible barriers often faced by Autistic people and families, so that every Autistic person can enjoy the same chance in society.

Our vision is for Ireland to be a country where every Autistic person is accepted as they are. Our purpose is to create an inclusive society for Autistic people that is accessible, accepting and affirming. We work to support the Autistic community and their families to fully engage in Irish life and build the capacity of society to facilitate true inclusion.

AsIAM’s work includes but is not limited to:

- Community Support Hubs (CSHs) (in person service)
- Information Line (phone, email and instant messaging service)
- National Supports (online and in-person offerings for adults and children)
- Accreditation and Training (for businesses, schools and communities)
- AsIAM Autism ID Card
- Employment and Over 18 Transitions
- Policy & Legal Advocacy
- Accessible Healthcare Programme

AsIAM operates across the following locations:

- Head Office, Blackrock, Co. Dublin
- CSH1 – Galway
- CSH2 – Dublin 8

Approximately 67 people are employed across the organisation. Employees operate under a hybrid working model with a mix of office based, site based and remote working arrangements.

0.2 Objectives of this RFT

The objective of this RFT is to appoint a qualified ICT Managed Service Provider (MSP) to provide Level 1, Level 2 and Level 3 support for all of AsIAM’s ICT systems and equipment in line with industry best practices. The MSP will be responsible for ensuring operational efficiency, service continuity and user satisfaction across AsIAM’s ICT environment, while also taking a proactive approach to maintaining strong cybersecurity, safeguarding systems and data and ensuring compliance with relevant standards and regulations.

Other key goals are to:

- Improve the user experience for remote access and file storage – supporting collaboration without compromising on security.
- Acquire/ upgrade hardware and software if required and configuration of any new systems and security requirements.

The Successful Tenderer should have capacity to take on the support service promptly, ideally by **1st September-October 2026**.

0.3 Current Situation

This section outlines the current ICT environment in terms of resources and support services. The detailed requirements to be addressed by tenderers are set out in the next section.

Tenderers should not assume that the existing setup represents the preferred or required configuration. Proposals for improvement are welcome.

0.3.1 Overview

AsIAM's ICT services are fully outsourced to a provider that currently manages the main office systems and end user equipment used by AsIAM, including ICT infrastructure in one of our premises (HQ).

Support services are currently supplied by Ekco (previously Radius).

Tenderers are not required to take over or continue operating the existing Ekco-hosted server infrastructure as-is; a proposed replacement (e.g. a cloud-first Microsoft 365 architecture) is acceptable, provided service continuity is maintained throughout transition.

0.3.2 Users

67 Users are supported using Windows laptops and operate hybrid working model.

These users are located at the following operational premises which must be supported:

- Head Office: Blackrock, Co. Dublin: 51 unique hybrid users (with c.a. 5 – 20 users present at any one time), Wi-Fi, managed printer, servers, meeting rooms – see 0.3.4 below
- Galway: 8 users, Wi-Fi and managed printer
- Dublin 8: 8 users, Wi-Fi and managed printer.

0.3.3 Support Arrangements

- IT support is delivered through a managed ICT service aligned with ITIL v4 principles
- The service provides end-to-end Level 1, Level 2 and Level 3 support across the full ICT estate
- Support is delivered through a hybrid model, combining remote support with onsite attendance as required.
- Core support hours are 09:00 to 17:00, Monday to Friday
- Identity and Access Management
 - Active Directory is used to manage user permissions and access controls.
 - Active Directory is synchronised with Entra ID to support hybrid cloud identity management.
 - Device and identity management supports secure access for office-based, remote and hybrid employees.

- Endpoint and Systems Management
 - All laptops and desktops are equipped with a remote management agent.
 - Technology support includes:
 - Remote monitoring and support
 - Patch management and security updates
 - Hardware health monitoring
 - Remote user assistance.
- No routine out-of-hours support is provided; any out-of-hours assistance is pre-arranged.

0.3.4 Remote desktop and S:Drive

Remote desktop is provided by the Tserver01 as noted in the Servers section below.

- The S drive is a shared drive hosted on the Domain controller.
- Various folders are shared via S drive with different permissions groups to ensure data security.
- For the purposes of costing and transition planning, Tenderers should assume that no existing data can be archived or excluded from migration; all data must be accounted for in the proposed file storage architecture.

0.3.5 Licence Management Arrangements

Ekco MSP manages AsIAM's Microsoft licences on their behalf. Licences are procured, administered and fulfilled through Microwarehouse, an authorised Microsoft Cloud Solution Provider (CSP). Ekco MSP is responsible for procurement and renewal of licences, assignment and reallocation within the Microsoft 365 tenant, ongoing monitoring and optimisation, day-to-day administration and support, and acting as the primary liaison with Microwarehouse and Microsoft. All licences are managed in accordance with Microsoft CSP and Not-For-Profit programme requirements.

0.3.6 Licence Ownership

All Microsoft licences are owned by AsIAM which operates as a Not-For-Profit organisation. Ekco MSP provides licence management services only and does not retain ownership, entitlement, or usage rights to the licences.

0.3.7 Licence Payment Arrangements

All licences are on an annual commitment and are paid monthly under Microsoft's Cloud Solution Provider (CSP) programme. Licence charges are processed via Microwarehouse, with applicable Not-For-Profit pricing and discounts applied by Microsoft.

Tenderers may propose Microsoft 365 licensing on either a monthly or annual commitment basis, whichever represents the most cost-effective solution while meeting AsIAM's needs as set out in this Appendix 1.

0.3.8 Current Microsoft Licences

Licence Type (Non-Profit)	Number of Licences Purchased	Number of Licences Assigned
Microsoft 365 Business Basic (Non-Profit)	6	6

Formatted: Normal, Indent: Left: 0 cm, First line: 0 cm

Formatted: Normal, Indent: Left: 0.12 cm, No bullets or numbering

Microsoft 365 Business Premium (Non-Profit)	80*	80
Microsoft 365 Business Standard (Non-Profit)	1	1
Microsoft Teams Phone Standard (Non-Profit)	24	23
M365 Teams Room Basic	1	1

* Current no. users = 67. Number of licences is higher due to annual minimum commitment.
AsIAM is switching to a monthly commitment from June 2026 onwards.

0.4 Technology Support

The following devices and resources are utilised:

Servers

- ~~Microsoft Windows Server 2019 Standard (4 vCPU, 12 GB RAM). Currently used as Domain Controller/File Shares, comprising: C: drive 100GB (49GB in use — used for server install and basic system data, not user data); D: drive (Data) 407GB (544MB free — used for the shared drives (S:Drive) for all of AsIAM). Microsoft Windows Server 2019 Standard (4 vCPU, 12 GB RAM, 400GB storage). Currently used as Domain Controller/ File Shares. Storage: 407 GB (95% full)~~
- ~~Microsoft Windows Server 2019 Standard (10 vCPU, 74 GB RAM, 926GB storage. Currently used as Remote Desktop Server. 1800 GB (99% full)). Currently used as Remote Desktop Server: 1.10TB storage (16.9GB free), holding AsIAM users' individual data.~~

Network

- Draytek 2866 firewall
- 2 x 24 port managed POE Ubiquiti UC Pro switches
- 4 x WiFi Access Points (UAP-AC-LR x2 and UAP-AC-Pro x2)
- Wifi (Virgin Media, Eir, Other)
- Managed printer.

End User Support

- 67 Windows-11 laptops (51 in HQ team, 8 in Galway office, 8 in Dublin 8 office)
- Microsoft Active Directory with Entra ID
- Microsoft Office
- Messaging: MS Outlook and Teams Chat (Internal only)
- Remote desktop environment with VPN (hosted by Ekco)
- Equipment support includes:
 - Device provisioning and setup
 - Configuration and patching
 - Fault diagnosis and repair
 - Remote and onsite user support
- Secure lifecycle management supports replacement and decommissioning of devices.

As part of the implementation programme (See Section 3), the MSP will optimise and modernise remote access, use of VPN and ensuring consistent performance for remote employees.

User Interface / Access:

Currently, end users have dual methods of accessing services:

- Desktop 1: immediately accessible upon logging onto laptop (synched with One Drive). All Microsoft applications are accessible in this environment without requiring the additional security of VPN.
- Desktop 2: remote desktop managed by IT Service provider. VPN required if outside of HQ. All Microsoft applications are accessible in this environment, except for video calls. U:Drive and S:Drive can only be accessed in this environment.

As part of the implementation programme (See Section 3), the MSP will provide end users with a single consistent user interface, i.e. eliminate the dual desktop setup and deliver one unified Microsoft 365-based workspace with no dependency on the legacy Remote Desktop environment. The MSP will also optimise Teams and SharePoint for collaboration, including structure, permissions and provide suitable training for all users.

System Protection

- Virus protection: Bitdefender
- Encryption: Bitlocker
- Device Management: Intune and some on Entra ID
- eMail filtering: Barracuda quarantine filtering

As part of the implementation programme (See Section 3), the MSP will review the system protection measures and update them as required.

File Storage

Two methods are currently in use which we wish to rationalise

- One Drive/ SharePoint (not formally structured/ requires strengthening)
- S:Drive cloud storage (hosted by Ecko)

As part of the implementation programme (See Section 3), the MSP will design and implement a unified file storage architecture including migration, permissions mapping, and user training.

Telephony / Voip

- Based on Yeastar Cloud using Linkus softphones with Full Teams integration
- Usage: via MS Teams integration or mobile phone app
- Call centre application for reporting and live stats = 8 licences
- Pre-recorded messages and call recording
- Number of phone numbers : 7 mainline numbers and 24 personal DDIs
- Number of user profiles: 26.

0.5 Current Volumes and Costs

0.5.1 Service Calls

The following illustrated the volumes of call over recent years.

Priority Level	2024	2025	2026 (to end-April)
----------------	------	------	------------------------

1	40	75	3
2	551	773	10
3	22	89	150
4	3	39	107
RRM*	9	29	1
Total	625	1005	271

* Remote Monitoring and Management

Notes:

- The increase in 2025 reflects (i) significant growth of the organisation in 2025 and (ii) persistent connectivity issues which have since been resolved. The 2026 figures represent the normal volumes of services calls.

0.5.2 Devices

Category	No. of
Switches	2
Firewalls	1
Access Points	4
Managed Printers	3

0.5.3 Current Costs

For information, the AsIAM's expenditure (after discounts and excluding VAT) in 2025 was:

Service	No. of	Cost per month
On site managed services	67	€975.00
Cloud Support	60	€1,800.00
Cloud Infrastructure	60	€740.00
Barracuda	84	€294.00
Bitdefender	65	€162.50
O365	109	€377.86
Phone System	22	€322.50
TOTAL:		€4,741.45

0.6 Estimations to Use for Costing and Sizing

The following estimates should be used by tenderers for purposes of planning and sizing their approach and costs. Actual figures may vary.

0.6.1 Service Calls

Tickets	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
P1	10	11	12	13	14	15
P2	30	34	36	40	43	45
P3	450	509	544	604	640	672
P4	300	339	363	403	427	448
Remote Management & Monitoring (RMM)	10	11	12	13	14	15
Total	800	904	967	1074	1138	1195

Note: Year 1 is based on 2026 figures to date. Years 2-6 based on % increase in users.

0.6.2 Users & Licences

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
Number of Users	79	89	95	105	111	117
Number of M365 Business Licences required	79	89	95	105	111	117

0.6.3 Telephony

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
No. VoIP Users	24	27	29	32	34	36
No. Mainline phone numbers	7	7	8	8	9	9
No. DDIs	24	27	29	32	34	36

0.6.4 PC Laptops to be Supported

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
No. PC laptops to be supported	79	89	95	105	111	117
Of which, new laptops to be provisioned	15	25	21	25	21	21

0.6.5 Other Equipment to be Supported

Equipment	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
Switches (HQ)	2	2	2	2	2	2
Firewalls (HQ)	1	1	1	1	1	1
Access Points (HQ)	4	4	4	4	4	4
Managed Printers (x3 locations)	3	3	3	3	3	3

0.7 Future Needs

The requirements stated in this RFT may be refined and adjusted in light of an initial planning/review exercise conducted with the Successful Tenderer. These may impact on the licences applicable, the services required, the ongoing support needed and in turn, costs.

Over the term of the contract, other changes – unforeseen at this point – may require to be addressed under the terms of this contract, for example:

1. Growth in numbers of users, devices, licenced products, data volumes, complexity or governance requirements.

2. Emergence of new threats or risks.
3. Compliance with new relevant standards, legislation or regulations.
4. Changes to the AsIAm's roles and responsibilities.
5. Replacement of components within the technology stack supporting the solution to remedy technical obsolesce (e.g. software going off support, absence of appropriate expertise).

How such requirements are dealt with will be addressed with the Successful Tenderer as part of the transition programme or the ongoing support service. AsIAm reserves the right (at its sole discretion) to seek other solutions or suppliers in such instances.

1 Services Required

The Managed Service Provider (MSP) will deliver a comprehensive ICT managed service covering the operation, monitoring, support and security of AsIAM's ICT environment. Services must align with ITIL v4, support a geographically distributed workforce and ensure systems remain secure, available, compliant and recoverable.

The MSP will act as AsIAM's primary ICT partner, providing Level 1–3 support, proactive management and continuous improvement across all ICT services.

For each set of services below, tenderers should confirm that they will deliver the service required and describe how they will do so. Any additional services or features provided within the quoted cost should also be described.

1.1 Infrastructure Management

- (a) Management and maintenance of all on-premise equipment and associated software.
- (b) Asset Register is maintained (devices provisioned/ repaired/ destroyed) and available to AsIAM.
Note: AsIAM does not currently hold a comprehensive asset register; this must be built and maintained by the MSP from the outset of the Term. Tenderers should describe their proposed approach to establishing and maintaining the Asset Register.
- (c) Software licence management: managing the procurement and allocation of licences and ensuring compliance with licensing obligations (AsIAM will own the licences).
- (d) On-site IT maintenance and support for infrastructure or complex issues.
- (e) Scheduled preventative maintenance and health checks for critical equipment.
- (f) Retirement or modernisation of the (Virtual) Remote Desktop Service as appropriate.

1.2 Managed Cloud & Hosting Services

- (a) Management of Microsoft 365 including Exchange Online, Teams, SharePoint, OneDrive and security configuration.
- (b) Optimisation of Teams and SharePoint for collaboration, including structure, permissions and training (where appropriate).
- (c) Administration of Entra ID, MFA, conditional access and identity lifecycle.
- (d) Monitoring of service health, performance and capacity.
- (e) Patch, update and release management.
- (f) Backup and recovery management including disaster recovery within agreed defined RPO/RTOs.
(No specific RPO/RTO values are prescribed by AsIAM; Tenderers should propose appropriate RPO/RTO targets based on best practice for Microsoft 365, cloud services, and AsIAM's operational profile, for agreement during Phase 1.)
- (g) Regular testing of recovery processes.
- (h) Availability target of ≥99.5% for core cloud services.
- (i) Alignment with Cyber Essentials (or equivalent) controls and recognised security standards.

1.3 User Experience

- (a) Users access a single, consistent workspace, avoiding the need to switch between multiple desktop environments - as is currently the case.
- (b) Workspace should be the Microsoft Licenced suite of tools, including managed MS Outlook Email, MS Teams, MS Office & Microsoft security features.

- (c) Users only have access to the systems and files that they are authorised to use.
- (d) Zero trust policy approach is experienced by users as supportive boundaries (i.e. by shifting compliance responsibility from users to centralised controls).

1.4 End-User & Device Support

- (a) Managed remote helpdesk for user support and troubleshooting.
 - Standard support to be available during working hours.
 - Ability to log support tickets (phone and email or online portal).
 - Tickets to be managed via an appropriate support system.
 - System should support audits and investigations that may arise (i.e. searchability of full ticket content or suitable alternative).
 - Availability of out-of-hours emergency support for approved emergency circumstances.
 - Clear escalation paths for support tickets with defined SLA times.
- (b) Level 1–3 support for laptops and all devices and software outlined above (with the potential to add mobile phones in future).
- (c) Device provisioning, configuration, patching and secure disposal.
- (d) Remote monitoring and management of all endpoints.
- (e) Support for hybrid working
- (f) Management of printers, peripherals and office ICT equipment.
- (g) Full ownership of incidents and service requests until resolution.
- (h) Remote access to laptops for troubleshooting and remote fixes.
- (i) Support for employees across Head Office, CSH1 Galway , CSH Dublin 8, and remote workers.
- (j) Laptop Repair:
 - End-user device break-fix service covering laptops.
 - Refresh policy for health checks/ replacement.
 - Robust disposal policy (i.e. end of life laptops can be returned with ease, destroyed securely, and destruction certificates provided).

1.5 Network & Infrastructure Support

- (a) Management of LAN, WAN and Wi-Fi infrastructure.
- (b) Support for firewalls, switches and access points.
- (c) Monitoring of network performance, availability and security.
- (d) Vendor liaison for connectivity and telecoms providers.
- (e) Maintenance of network documentation and asset registers.
- (f) Support for multi-site connectivity and secure remote access for outreach employees.

1.6 Telephony & Communications

- (a) Management of Teams-based telephony.
- (b) Support for IVR, call routing, call recording.

1.7 File Storage

- (a) Management of the centralised managed file storage system – as established in the Implementation programme – including:
 - File / folder structures
 - Role-based access rights

- Backup and restore
 - Collaborative working arrangements (e.g. sharing documents)
 - Audit trails of access, additions, deletions
- (b) Managing AsIAM's obligations and commitments around Information Security and GDPR. This includes appropriate confidentiality, access controls and integrity of data – to avoid unavailability, unauthorised access, unnecessary duplication, excessive retention, loss of data, or other data breaches. The MSP must design a new folder structure, implement role-based access, and ensure GDPR-aligned retention and deletion
- (c) Monitoring of storage capacity and managing any reorganisations or increases required in capacity.

1.8 Cyber Security

1.8 Active security monitoring services (e.g. SOC or SIEM) are not a mandatory requirement of this RFT; the controls listed below represent the required baseline. Tenderers may propose SOC/SIEM services as an optional enhancement under Section 1.11 (Optional/Drawdown Services) with associated pricing included in the Optional/Drawdown Services section of the Pricing Schedule (Appendix 2).

Formatted: Normal

- (a) Implementation and monitoring of security controls aligned to Cyber Essentials and ISO/NIST principles, covering all devices, systems and user accounts.
- (b) Centralised zero-trust security architecture with automated policy enforcement.
- (c) AsIAM systems/ accounts can only be accessed by authorised users on authorised devices.
- (d) Appropriate security measures are in place for remote access/ work from home where Wifi access cannot be controlled (e.g. VPN).
- (e) Where possible, AsIAM third party apps/ software can only be accessed via authorised MFA, including but not limited to: mobile application, mobile phone number and email address.
- (f) Dark Web Monitoring.
- (g) Have Geo-blocking to allow blocking of access from IPs outside Ireland / UK / EU.
- (h) Vulnerability scanning and remediation.
- (i) Incident detection, response and reporting.

1.9 Data Management & Security

- (a) Encryption of data in transit and at rest.
- (b) All data stored within the EU and ideally, in Ireland.
- (c) Role-based access control and privileged access management.
- (d) Logging, alerting and threat monitoring.
- (e) Enhanced protection of special category data processed in service delivery.
- (f) Support for safeguarding-related data governance requirements.

1.10 Service Management & Governance

- (a) ITIL-aligned incident, problem, change and request management.
- (b) Clear definition of the roles and responsibilities of the MSP and of AsIAM in a RASCI chart.
- (c) Clear visibility for AsIAM of all incidents.
- (d) Provision and maintenance of suitable documentation for AsIAM to operate the service and equipment (e.g. operating manuals, user guides, training materials, backup/recovery procedures).

- (e) Monthly service reporting, KPI/SLA tracking and trend analysis.
- (f) Annual service review and continuous improvement planning.
- (g) Dedicated Account Manager and escalation path.
- (h) Support for audits, compliance checks and funding-related reporting.
- (i) Exit Plan: support for transitioning to a new MSP.

1.11 Optional / Drawdown Services

- (a) Project delivery, cloud migrations and infrastructure upgrades.
- (b) Cyber security enhancements and training.
- (c) Consultancy on ICT strategy, risk and compliance.
- (d) Additional resources at agreed day rates.

2 Resources & Skillsets

This section seeks information about the tenderers capacity to provide the services required.

2.1 Resources

Tenderers should describe their capacity to deliver the services satisfactorily over the contract term. This should include details of the roles, skills and qualifications available to support service delivery.

Tenderers identify any roles delivered by subcontractors and confirm how continuity of service is assured.

2.1.1 Service Organisation

Tenderers should describe how their service organisation is structured and how it fits into the overall management structure. Measures to keep processes and technologies up to date and to keep employees' skills updated should be described.

2.1.2 Mandatory Roles (Must Have)

Tenderers should detail the numbers of employees that can fill the following roles and their range of qualifications relevant to the role:

- Service Delivery Manager / Account Manager
- Service Desk Analyst (Level 1)
- Technical Support Engineer (Level 2)
- Senior Technical Engineer / Infrastructure Engineer (Level 3)
- Network Engineer
- Equipment Engineer (Laptops, servers, printers)
- Telephony / MS Teams specialist
- Security Lead / Security Specialist.

2.1.3 Desirable Roles (Desirable)

Tenderers should detail the numbers of employees that can fill the following roles and their range of qualifications relevant to the role:

- Cloud / Azure Specialist
- Endpoint Monitoring Specialist
- SharePoint / Collaboration Specialist
- Cyber Security Analyst
- Transition / Onboarding Manager
- Training / Adoption Specialist.

2.2 Service Team

Tenderers should detail how they will fill the key roles/responsibilities in the service team and provide CVs for the principal roles in the team, e.g.

- Service Delivery Manager / Account Manager
- Technical Lead / Senior Engineer (Level 3)
- Security Lead / Security Specialist
- Service Desk Manager / Lead.

3 Implementation Programme

The Successful Tenderer must deliver a structured implementation programme that modernises AsIAM's ICT environment, resolves legacy issues and transitions the organisation to a unified, secure, cloud-first operating model. The programme must ensure continuity of service, minimal disruption to users and full alignment with AsIAM's operational, security and accessibility needs.

The programme will be conducted on phased basis as outlined below. The Gantt Chart represents lapsed periods for each phase and assumes that work will spread over this time period rather than being a full-time commitment on the party of the MSP or AsIAM. Tenderers must provide pricing for all phases. AsIAM may change the timing or sequence of phases and may draw down phases at its sole discretion; pricing for all phases does not represent a commitment by AsIAM to proceed with any or all phases. Tenderers should cost for all phases but AsIAM may change the timing or sequence of phases and this does not represent a commitment to go ahead with all phases.

Phase	Phase Title	Week 1-4	Week 5-8	Week 9-12	Week 13-16	Week 17-20	Week 21-24
1	Transition, Discovery & Stabilisation						
2	Unified User Workspace & Identity Modernisation						
3	File Storage Consolidation & Collaboration Improvements						
4	Remote Access & Network Modernisation						
5	Security Hardening, Decommissioning & Optimisation						

Phase	Phase Title	Weeks (From/To)	Key Tasks
1	Transition, Discovery & Stabilisation	1–4	Controlled handover; discovery of systems; validate assets/licences; establish governance; stabilise issues.
2	Unified User Workspace & Identity Modernisation	4–10	Implement solution for: dual-desktop; modernise identity; implement MFA/Conditional Access; deliver unified Microsoft 365 workspace
3	File Storage Consolidation & Collaboration Improvements	6–14	Design consolidated storage; migrate U:Drive/S:Drive; implement role-based access; improve Teams/SharePoint collaboration by implementing stricter sharing rules to protect confidential files.
4	Remote Access & Network Modernisation	8–18	Modernise remote access; reduce VPN/Remote Desktop dependency; upgrade network hardware; improve multi-site connectivity.
5	Security Hardening, Decommissioning & Optimisation	10-24	Implement Cyber Essentials controls; deploy Zero Trust; enhance monitoring;

Phase	Phase Title	Weeks (From/To)	Key Tasks
			decommission legacy systems; continuous improvement plan

3.1 Phase 1 — Transition, Discovery & Stabilisation (Weeks 1–4)

The MSP will assume operational responsibility and establish a complete understanding of the current environment.

Key Tasks

- Controlled handover from the incumbent MSP, including all documentation, credentials, configurations and ticket history.
- Full discovery of: servers, network, Wi-Fi, firewalls, RDS, file storage (existing S:Drive as well as SharePoint/OneDrive folders), identity management, telephony, devices and assistive technologies.
- Migration of Telephony systems with minimal disruption.
- Validation of asset registers, licensing and security posture.
- Establish service governance, reporting, escalation paths and communication channels.
- Immediate stabilisation of any critical issues.

Deliverables

- Transition Completion Report.
- Validated asset and configuration baseline.
- Service governance framework in place.

3.2 Phase 2 — Unified User Workspace & Identity Modernisation (Weeks 4–10)

AsIAM currently operates two desktop environments. The MSP must deliver a single, consistent Microsoft 365-based workspace.

Key Tasks

- Eliminate the dual-desktop model and remove dependency on the legacy Remote Desktop Server (unless required temporarily).
- Implement modern identity and access management (Entra ID, MFA, Conditional Access, Zero Trust).
- Ensure users access all applications through one unified interface.
- Provide training and onboarding materials.

Deliverables

- One unified user workspace
- Updated identity lifecycle processes
- User training and support documentation

3.3 Phase 3 — File Storage Consolidation & Collaboration Improvements (Weeks 6–14)

AsIAM currently uses two separate file storage systems. The MSP must consolidate these into a single, secure, role-based storage model.

Key Tasks

- Analyse current folder structures, permissions, duplication and retention issues.
- Design a consolidated SharePoint/OneDrive architecture.
- Implement role-based access and GDPR-aligned retention.
- Migrate data from U:Drive/S:Drive to the new structure.
- Improve Teams/SharePoint collaboration workflows, including stricter file sharing permissions to allow for better security of confidential files.
- Provide user training.

Deliverables

- One unified file storage system.
- Clean folder hierarchy and permissions model.
- Migration completion report.

3.4 Phase 4 — Remote Access & Network Modernisation (Weeks 8–18)

Remote access must be modernised to support hybrid working and reduce reliance on VPN/Remote Desktop.

Key Tasks

- Implement modern remote access solutions with secure cloud-based access.
- Reduce or eliminate VPN dependency when working remotely.
- Review and upgrade network infrastructure (firewalls, switches, Wi-Fi), replacing end-of-life equipment. Ensure that infrastructure is consistent across the three AsIAM sites.
- Implement secure multi-site connectivity and improved Wi-Fi performance.
- Update network documentation.

Deliverables

- Modern remote access solution.
- Updated network infrastructure.
- Improved performance for remote and on-site users.

3.5 Phase 5 — Security Hardening, Decommissioning & Optimisation (Weeks 10–24)

Security improvements must be implemented early and continue throughout the programme.

Key Tasks

- Implement Cyber Essentials-aligned controls and Zero Trust architecture.
- Deploy geo-blocking, dark web monitoring, vulnerability scanning and enhanced logging.
- Strengthen privileged access management and encryption.
- Decommission legacy systems (RDS, old storage, unused apps).
- Conduct post-implementation review and deliver a continuous improvement roadmap.

Deliverables

- Full Cyber Essentials alignment.
- Decommissioning report.
- Final optimisation and continuous improvement plan.

3.6 Approach

Tenderers should describe their approach to the programme and their experience of conducting similar programmes, describing each phase and their experience of similar programmes.

Tenderers should note that the phase timelines in Section 3 reflect an indicative sequence assuming part-time engagement from both MSP and AsIAM project resources with some overlap between phases. Proposed timelines that are significantly more demanding on AsIAM's resources than this assumption will attract lower scores.

3.7 Project Plan

Tenderers are required to submit a sample Implementation Plan as part of their response, demonstrating how they will achieve a controlled, orderly and low-risk transition. The successful tenderer must engage fully with the AsIAM and the current service provider to ensure continuity of service and secure transfer of all relevant information, documentation and operational knowledge.

Tenderers must also include:

- The main activities involved.
- The expectations in terms of inputs expected from the AsIAM should be set out clearly and minimal.
- Details of how transition risks will be identified, managed and escalated.
- Full disclosure of all transition costs clearly itemised in the Pricing Schedule.

3.8 Project Team

Tenderers should describe their project team structure and who will fill the following roles, some of which might be combined. Tenderers should confirm that the named resources will be available to undertake the project.

- Project Manager.
- Technical Lead / Solution Lead.
- Other key personnel.

Where roles are being filled by a third party or contractor, this should be stated.

4 GPP/Sustainability

This section sets out the requirements regarding Green Public Procurement in relation to the delivery of the services required in the tender.

Tenderers are asked to describe the measures that they (and any key partners) are taking to comply with the EPA's "Irish GPP Criteria: ICT Products and Services"

(See: www.epa.ie/publications/circular-economy/resources/EPA_GPP_Criteria_ICT_2024.pdf), notably in the areas of:

1. Energy efficiency
2. Resource efficiency
3. Longevity
4. End-of-life considerations
5. Sustainable policies and practices along with relevant certifications.

in respect of their (1) hosting service and (2) business operations.

5 Cost

5.1 Cost Breakdown

Tenderers are required to set out in detail the cost elements of the total cost over the term of the contract - and subject to the cost increases envisaged in section 2.10.6 of the RFT - that are needed to deliver the requirements. All costs should exclude VAT but the VAT rates applicable should be provided.

The cost details should be provided using the Pricing Schedule Excel workbook (Appendix 2) available on eTenders. The "Total Supply & Support Cost" will be the basis for scoring the Costs award criterion as described in section 3.3.1 (Step 2) of the CFT. In evaluating the Award Criteria, higher marks will be given to tenderers that justify these costs and provide the highest level of detail in the corresponding sections of this RFT.

The price must cover all requirements that will be delivered to include inter alia:

Ongoing Support Service

- Ongoing support and maintenance of the devices and software including Service Management
- Ongoing Subscriptions and other SaaS-type charges.

Implementation Programme

- Provision of the solution, the hosting service and other operational costs
- Services to setup, manage and administer the devices and software
- Provision of the licences necessary to build and operate the service
- Setup/configuration/testing of the proposed solution
- All implementation services.

Discounts offered or 'pro bono' time based on AsIAM's charity status.

5.2 Pricing Structure

(a) Tenderers must provide details of their pricing model (e.g. basis for prices, pricing packages, discounts, etc) and any options available.

(b) Any add-on or complementary products should be listed and pricing information provided.

~~(b)~~(c) Tenderers must clearly state the mechanism by which pricing will be adjusted as user numbers, devices or service volumes increase over the Term (e.g. per-user, per-device, or tiered pricing), based on the volumes set out in Section 0.6. Any such mechanism must be transparent, predictable and consistent with the Pricing Schedule (Appendix 2).

5.3 Additional Services

Tenderers should submit hourly rates (excluding VAT) for additional services that they offer for different categories of personnel and their experience level. The AsIAM reserves the right to seek a fixed fee for any additional services at its discretion.