



Microsoft Intune and Autopilot

Service Definition

Contents

Solution Overview.....	2
Key Features.....	2
Key Benefits.....	2
Objectives of the Service	3
Service Transition.....	3
Project Roles & Responsibilities	4
Project Documentation.....	5
Managed Service	5
Service Desk	6
Classification and Prioritisation	6
Self-Service	7
Customer Success Management	7
Data Protection & GDPR.....	8
Why Partner with Atech?	9
Credentials and Capability.....	9
Microsoft Endorsements and Specialisations	9
Security and Compliance	10
Exit Planning	11

Solution Overview

What is Intune?

Microsoft Intune is a cloud-based endpoint management solution. It controls how users access organisational resources and makes it easier to manage apps and devices across your various devices, such as mobile devices, desktop computers, and virtual endpoints.

Mobile devices/BYOD practices pose a challenge for IT administrators, who need to manage various devices, both on/off-site, with equal access to information, but also protect data security. Iomart offers Microsoft Intune to create a single IT system, enabling remote and secure control of all devices, without the costly infrastructure that other traditional management solutions rely on.

Iomart can assist organisations to get the best out of existing licencing and provide recommendations based on requirements.

Key Features

- Intune readiness and configuration assessment
- Endpoint security review and compliance validation
- Windows Autopilot setup for zero-touch deployment
- Policy and profile configuration for all devices
- Licensing optimisation and cost-efficiency recommendations
- Optional managed service for continuous endpoint support
- Application deployment and update management for all devices
- Device compliance automation with Conditional Access
- Security baselines and hardening configuration
- Endpoint analytics setup for performance and health insights

Key Benefits

- Delivers secure, scalable device management for all endpoints
- Enables faster onboarding with zero-touch provisioning capabilities
- Improves compliance and governance across managed devices
- Optimises use of existing Microsoft licensing for cost efficiency
- Enhances user experience for remote and hybrid working environments
- Reduces security and compliance risks through proactive monitoring
- Provides a future-ready endpoint strategy aligned with organisational needs
- Cuts manual effort using automated device workflows and policies
- Offers greater visibility of device health and performance trends
- Strengthens protection against endpoint threats and vulnerabilities effectively

Objectives of the Service

Key objectives of the service are:

- Expert knowledge around the implementation/best practice when configuring Microsoft Intune.
- Enable organisations to manage devices in a more effective/cost-efficient manner.
- Assist your organisation to be compliant with device regulatory standards such as Cyber Essentials Plus.
- Maximise Efficiency, streamline process around application management and device provisioning.
- Single pane of glass to simplify management.
- Cost effectiveness, using features like Intune Autopilot for device provisioning, removing the need for in place infrastructure for device deployment.
- Secure by design to meet the latest NCSC/NIST device guidelines.

Service Transition

As a Managed Services Provider, customer satisfaction is of the utmost importance to Iomart and as such, a positive and successful Service Transition stage is paramount. The Iomart project approach is based on the PRINCE2 framework, and we also recognise that modern technology transformations rely on the ability to remain responsive and offer agile and practical solutions. All projects are comprised of three high-level milestones:



Our approach is underpinned by a strict adherence to proven project and risk management methodology and techniques that ensure that Iomart can meet customer objectives to budget, in a timely manner and mitigate the risks associated throughout.

Project Roles & Responsibilities

Role	Responsibilities
Project Manager	Manage overall delivery of the project Provide leadership and guidance to the project team First point of contact for during the project Daily/Weekly status updates to all stakeholders throughout the project Manage third parties and their responsibilities Project Governance Manage RAID log (Red-Amber-Green, RAG, Status) Manage and maintain the Project Plan Communication management Quality assurance throughout the project Change Management Risk management Monitor and manage Iomart resources for delivery Delivery of Project documentation – knowledge transfer
Account Manager	Monitor and review any changes proposed and discuss any commercial impact
Solution Owner/ Solution Architects	Design Lead throughout all stages of the project
Lead Deployment Engineer (Deployment team)	Lead all deployment and build activities throughout the project Manage and coordinate other deployment engineers, network team and any subject matter experts required
Service Delivery Manager	Support onboarding to business as usual Customer point of contact for service delivery Benefits realisation
Subject Matter Experts	Provide guidance and knowledge to Project team Support Lead Deployment engineer in deployment/build phase

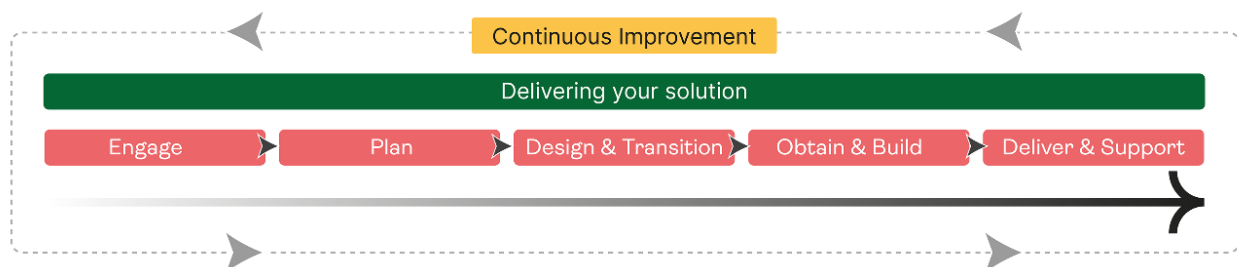
Project Documentation

Throughout the project, Iomart will utilise and deliver key project documentation, to ensure successful and regular communication. Documentation could include:

- Project Plan
- Project Initiation Document
- User Acceptance Testing Plan and Sign Off
- Platform documentation
 - RAID log, RAG rated, highlighting:
 - the **R**isks associated with the delivery and mitigating actions
 - the tracked **A**ctions ensuring it's clear who's doing what
 - the **I**ssues that are monitored and progressed to resolution where possible
 - any project **D**ependencies
- Meeting minutes from internal/external meetings
- Weekly highlight reports to show continual progress, highlights, and lowlights
- Change request documentation when managing the overall scope of the project
- Project closure documentation
- Customer Handover Document and Welcome Pack

Managed Service

Iomart use a set of clearly defined stages that are aligned to ISO 20000-1 and ITIL service management frameworks. This structure means you will get a consistent and reliable experience throughout your partnership with us.



The main benefits of our managed service are:

- Access to vendor accredited staff
- 24x7x365 ITIL-aligned service desk supporting Event Management, Incident Management, Request Fulfilment, Patch Management, and Change Control.
- Clear response KPIs based on ticket classification and severity.
- Optional access to Service Delivery Managers who will support the customer with continual service improvement, capacity management, and change co-ordination.
- Access to service desk support, billing, and configuration management via the Iomart Control Panel or phone.

Service Desk

The Iomart service desk is audited and compliant to ISO 20000-1 and ISO27001 standards and brings together over 100 technical operations staff based in the UK. Customers can contact our service desk on a 24x7 basis via:

- Iomart Control Panel – Authorised users will be given access to the panel to raise tickets; they will also be able to see progress on raised tickets and view additional account information.
- Telephone – Customers can call to get in touch directly with an engineer who can assist in escalating or raising a ticket with our support teams.

Classification and Prioritisation

Our managed services prioritise regular communication between Customers and Iomart. Service Desk teams are performance managed against these metrics.

There are three types of ticket Customers can raise when in need of support. And can raise three types of tickets:

- Incident
- Service Request
- Change Request

Iomart prioritise incidents using the following severity levels:

Priority	Description	Response Time	Resolution Target*
Priority 1 (Critical)	Critical issues where multiple users are unable to work, and the business is put at risk.	30 Minutes	4 Hours
Priority 2	High-priority issues detrimentally impacting a business unit or function.	1 hour	8 Hours
Priority 3 – DEFAULT	Issues impacting a small group of users or an individual user which affects their ability to work.	2 Hour	16 Hours
Priority 4	Low-priority issues which have no immediate impact on client's ability to work.	3 Hours	48 Hours
Priority 5	Information/Service Requests – Request for information, Additions to services etc.	4 Hours	5 Business Days

Service requests and Normal changes are treated as Severity 4 and Emergency Changes as Severity 1.

Self-Service

In addition to our service desk, we can offer you access to our self-service dashboard which offers the ability to:

- View billing information.
- View invoices and payments.
- Report incidents and monitor previous support tickets.
- Raise new service requests and monitor previous requests.

All these facilities are available through a single webpage. Access using new Control Panel Accounts can be requested from your Account Manager.

Customer Success Management

Your Customer Success Management provides a point of ownership for your operational relationship with Iomart, and all day-to-day matters relating to the delivery and performance of the services.

Management Component	Definition
Customer Success Management (CSM)	Your nominated Customer Success Management will work to: Agree the frequency and agenda of service performance review meetings, and chair these meetings, Provide periodic service performance reports, identifying agreed service compliance, analysis, and trends over the preceding periods, Provide and maintain a Service Improvement Plan, and review progress on the agreed initiatives and actions with you, Provide escalation support and communications as required and in accordance with Iomart's Escalation procedures, Organise and participate in the Service Governance process and manage all agreed in-scope changes to the Services and documentation. Present and review Iomart's standard operating policies and procedures on request and as set out within Iomart's Operations Manual. Continually explore new innovations or potential improvements to the Service that the parties may wish to adopt.

Data Protection & GDPR

Atech, part of the Iomart Group, is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. Our Data Protection policy sets forth the expected behaviours of Iomart Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an Iomart Contact (i.e. the Data Subject). Iomart, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in our Data Protection policy (available on request).

Iomart's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Iomart Employees and Third Parties to share in this commitment.

Iomart uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Iomart Entities.
- To provide services to Iomart customers.
- The ongoing administration and management of customer services.
- The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

Each Iomart Entity will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Iomart will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject prior to entering a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party.

Why Partner with Atech?

Credentials and Capability

Atech is the one of the UK's most accredited providers of secure hybrid cloud managed services, delivering deep expertise across Microsoft technologies, data protection, and cybersecurity. We hold Microsoft designations for **Modern Work, Security, Infrastructure (Azure)** and are recognised as an **Azure Expert MSP** – a status achieved by only 60 partners globally and 15 in the UK.

As part of the Microsoft AI Cloud Partner Program, we have validated technical capabilities across the full cloud lifecycle. Our inclusion in the **Azure Expert MSP Program** reflects proven excellence in people, processes, and tools, ensuring sustainable, repeatable, and scalable managed services. This means you can rely on a partner that consistently delivers best practice and operational efficiency.

Partnering with us gives you access to over **200 Microsoft cloud specialists**, including **two Microsoft MVPs**, ensuring unparalleled technical depth and experience.

Microsoft Endorsements and Specialisations

We hold multiple Microsoft Solutions Partner designations, including:

- Digital & App Innovation (Azure)
- Data & AI (Azure)
- Business Applications



Figure 1: Microsoft Accreditations

In addition, we have achieved advanced specialisations in areas such as:

- Cloud Security
- Identity and Access Management
- Threat Protection
- Infra & Database Migration
- Azure Virtual Desktop
- Enterprise Application Migration to Azure



Figure 2: Microsoft Designations

These credentials validate our ability to deliver complex, secure, and innovative solutions aligned to Microsoft best practices.

Security and Compliance

Security is at the heart of our services. Atech is **ISO 27001 certified**, **Cyber Essentials Plus accredited**, and a member of the **Microsoft Intelligent Security Association (MISA)** – an invitation-only program granting access to Microsoft's top security experts. We also hold **CREST accreditation** and participate in the **Microsoft MSSP Program**, one of only 12 partners in the UK, giving our customers direct benefits such as access to product teams and funded workshops.

Further reinforcing our security leadership:

- **Microsoft Gold Partner Status** alongside **Azure Expert MSP**
- **Microsoft MSSP Program** (1 of only 12 UK partners)
- **Microsoft Fastrack Ready Partner** (1 of only 300 globally)
- **Microsoft XDR status**

These credentials provide you with assurance that security is embedded throughout design, migration, and ongoing management. Combined with our advanced specialisations and industry recognition, they demonstrate our ability to deliver secure, compliant, and future-ready solutions.

Exit Planning

If you wish to transition to an alternative supplier, Iomart will work with you and the new supplier to ensure an efficient and seamless transition. Like our implementation process, our exit process will ensure that all stakeholders are engaged, risks are identified and mitigated, and that a clear programme of works is documented and communicated.

Upon confirmation of transition, Iomart will engage with you to create a Statement of Work and present a services package that will ensure a successful move.

The topics to be discussed include:

- Data migration
- Simultaneous use (if needed)
- Handover of projects in progress (if applicable)
- Final period report(s)
- Final period invoice(s)

You can be assured of minimal disruption during the transition, therefore allowing you to focus on business-as-usual activities.

Please see our Terms and Conditions for further detail.

ATECH IOMART

6 Atlantic Quay, 55 Robertson Street, Glasgow, G2 8JD