Elysian:IT

Microsoft Solutions Partner

CYBER ESSENTIALS PLUS

nqa ISO 27001 INFORMATION SECURITY MANAGEMENT

G-Cloud 15

Microsoft 365 Security Baselines Implementation

January 2026

01256 976 650
info@elysianit.com
www.elysianit.com

Follow

Acknowledgements

Thank you to everyone who has given their time and effort to meet us and provide the information that this document is based upon.

Point of Contact

For further information regarding the contents of this document, then please contact the following nominated contact:

Bid Team
bid.team@elysianit.com
+44 1256 976650

Copyright

Confidentiality

Contents

1. Service Definition - *providing clarity and transparency*

ElysianIT Offer a Range of Services related to Microsoft 365 (Office 365) which build into a complete Service offering:

Microsoft 365 - Readiness and Assessment
Microsoft 365 – Health Check
Microsoft 365 - Roadmap and Strategy
Microsoft 365 - Performance Testing and Quality Assurance
Microsoft 365 - Baselines Implementation and Pilot
Microsoft 365 - Implementation and Enhancement
Microsoft 365 - Migration
Microsoft 365 - Project and Change Management
Microsoft 365 - Security Audit and Recommendations
→ Microsoft 365 - Security Baselines Implementations
Microsoft 365 - Security Enhancements
Microsoft 365 – Support
Microsoft 365 – Guidance Documentation, Training and Coaching
Microsoft 365 – Tenant to Tenant Migration

Our "Microsoft 365 – Security Baselines Implementations Service" is a service whereby we deploy our standard security setup to your Microsoft 365 Tenant. The deployment has been designed to use the Microsoft Best Practices guidance and our real-world experiences. The objective of this service is to provide an accelerated deployment of security best practices to your Tenant.

The following table provides the Microsoft 365 (M365) product overview which are services used by this engagement.

Identity and Access Management	Device Management	Data Governance	Threat Management
Office 365 (E1\E3) Logon Identities (SSO), Security and Privacy (Password Policies, external sharing), Identity Protections (MFA and Password Reset. OneDrive\SharePoint\Teams\Skype Sharing and Syncing restrictions and Exchange Mail Flow, Transport Rules, Compliance Management, S/MIME, TLS, Protection and Mobile Access	**Office 365 (E1\E3) - Active Sync** Device Access Management, Full Device Wipe, Device Security Enforcement	**Office 365 (E1\E3)** Data Classification, Data Retention, Data Loss Prevention, Sensitive Information Types, Labels and eDiscovery	**Office 365 (E1\E3)** Includes Exchange Plan 1, Office Message Encryption Portal and in-built anti-malware detection for non Exchange Apps (SharePoint\Teams\OneDrive) **Exchange Plan 1** Anti-Spoofing, Anti-Malware, Anti-Spam, Mail Flow, Transport Rules
Active Directory Premium Plan 1 (EMS E3) Password write-back to on-premise AD, Advanced MFA (On-Premise and SaaS based solutions), MIM Licensing, Conditional Access, Windows 10 Bit locker Management	**Office 365 (E1\E3) - MDM** Enhancement to Active Sync, Full Wipe and Selective Wipe, Device Policies and Compliance	**Azure Information Protection Plan 1 (EMS E3)** Advanced Data Classification, File Protection (Encryption), Visual Document Marking supports Office 365, File Shares and User Local Locations	**Office Threat Intelligence (O365 E5)** Dashboard which provides a holistically view of the Threat landscape, Attack Simulator and Threat Tracker
Active Directory Premium Plan 2 (EMS E5) Risk-Based Sign-In and Advanced Reporting	**Intune with ADP1 (EMS E3)** Advanced Mobile Device Management, Mobile App Management, Enhancement to Office 365 MDM and Active Sync and PC Management	**Azure Information Protection Plan 2 (EMS E5)** Advanced AIP1, Auto classification	**Azure Information Protection (EMS E3)** Advance support for Office Message Encryption Portal, SharePoint IRM
Office Advanced Compliance (O365 E5) Lockbox - Microsoft Support Just In-Time Privilege Access to tenant data, control how a Microsoft support engineer accesses your data during a help session		**Office Advanced Compliance (O365 E5)** Auto Data Classification, Policy based governance and Advanced eDiscovery	**Office ATP (O365 E5)** Unknown malware attachment detections, Safe email links, works with Exchange, Office Pro Plus, and document libraries (SharePoint\Teams\OneDrive)
Office 365 Cloud App Security (O365 E5) Gain enhanced visibility and granular security controls and policies including the ability to monitor Risk Based sign in (similar to ADP2) block access to unmanaged cloud applications.		**Office 365 Cloud App Security (O365 E5)** Enhanced Data governance, Supports AIP and Sensitive Types, Centralized Dashboard, email and text alerts, manual firewall log review	**Defender ATP (Win E5)** Abnormal and Behavioral Activity Detection, IOC, AD, SIEM integration, Windows 10, Mac, Linux, Windows Server, iOS and Android support
Microsoft Cloud App Security (EMS E5) Advanced Office 365 Cloud App Security support for third-party SaaS solutions, Firewall log Automation, suspend user access, apply AIP policies and Session Proxy App (requires Azure AD Premium plan 1)		**Microsoft Cloud App Security (EMS E5)** Advanced Office 365 Cloud App Security support for third-party SaaS solutions, Firewall log Automation, suspend user access, apply AIP policies and Session Proxy App (requires Azure AD Premium plan 1)	**Azure ATP (EMS E5)** Abnormal and Behavioral Activity Detection (pass the hash),monitors on-premise and IaaS environments, integrates with Office ATP, Defender ATP and Office Threat Intelligence and SIEM integration
			Office Cloud App Security (O365 E5) Monitoring and Reporting of impossible login and abnormal and behavioral activity
			Microsoft Cloud App Security (EMS E5) Same as Office CAS, but can support Third-Party SaaS Solutions.

More information on the Microsoft 365 Product features please see section 1.2.

1.1 Service Features

The following features are elements of this service:

The Microsoft 365 Security baseline deploys security standards into your existing or new Microsoft 365 tenant covering the common elements of the deployed service we call this out Zero-to-Hero Security baseline.

The Zero-to-Hero security baseline is made up from the CIS Benchmark, NCSC Guidelines, Microsoft 365 secure score and our industry standards.

This engagement can cover all Microsoft 365 services and third-party connected services such as:

- Exchange Online Protection
- SharePoint, MS Teams and OneDrive
- ActiveSync Quarantine
- Defender XDR
- Defender for Office 354
- Endpoint Manager MAM and MDM (aka Intune)
- Entra ID (including Entra ID Connect, Entra ID Conditional Access, Entra ID PIM, Windows AD DS)
- Okta, Proofpoint, Mimecast, One Login, Darktrace, zScaler and other ISV products
- Data Loss Prevention
- Data Classification

Before the commencement of this service, we will agree on the solutions areas and associated costs for this engagement.

This service can be used in conjunction with our other services to deliver a complete programme of work.

1.2 Microsoft 365 Product Features

The following are features of Microsoft 365 (Office 365) and other connected third-party solutions

1.2.1 Identity and Access Management

Identity and access management focuses on the security control plane to access Microsoft online services, on-premise solutions and third-party SaaS based solutions (Salesforce, ServiceNow etc..).

Enhance security and compliance – Redefine your approach to security with conditional access policies and multi-factor authentication (MFA) that mitigate risk without disrupting valid users. Reduce the attack surface by limiting privileged accounts and reviewing access rights

Identity and access management typically covers the following products: Azure AD, Azure AD Premium, Azure AD Privilege Identity Management (PIM), Azure AD Conditional Access (CA) but might also cover third-party solutions such as Okta, One Login, Windows AD CA (PKI), Windows CALs and Windows AD DS

1.2.2 Device Management

With Device Management, people can work securely from the phone (iOS, Android), tablet (iOS, Android), Mac, Linux, or Windows —whether it's corporate-owned, employee-owned, or a third-party managed device.

Control access to your critical corporate data with policies that you define based on conditions such as user, location, or device state. As conditions and risk change, the controls you set keep your data safe in real time.

Safeguard your apps and data both before and after access with a rich set of app protection policies, such as the ability to restrict copy/paste and save-as. No device enrolment required: you can enforce app policies even on personal devices.

Device Management typically covers the following products: Microsoft Endpoint Managed (MEM), Microsoft Endpoint Configuration Manager (MECM), Autopilot but may also cover third-party solutions such as Zoho ManageEngine Desktop Central

1.2.3 Data Governance

Data Governance in the security context can provide the following:

- **Compliance Manager** is a dashboard which looks at the entire organisation to make sure that the policies instituted are being followed through real time auditing for analysis and corrective action. You can monitor email communications and data stored within Office 365 and content in third-party solutions.
- **Cloud App Security** allows organisations to set up anomaly detection policies, so you can be alerted to potential breaches of your network. Anomaly detection works by scanning user activities and evaluating their risk against over 70 different indicators, including sign-in failures, administrator activity and inactive accounts
- **Classification and Labels** in Office 365 can help you take the right actions on the right content. With labels, you can classify data across your organization for governance, and enforce retention rules based on that classification.
- **Advanced eDiscovery** can search multiple data sources and provide relevant results based on the search. You can also import the searchable content into Office 365. Advanced eDiscovery employ

optical character recognition for content within pictures and analyses email threads to recognise near duplicate content. You can tag individual documents with key words to enhance future search results as well. What may have taken weeks or months in the past can be significantly condensed.

Data Governance typically covers the following products: Microsoft Compliance Center, DLP, Microsoft Cloud App Security, Azure Information Protection (AIP), Labels and Retention, but might also cover third-party solutions such as Ernst & Young (EY) data solutions, Mimecast, Darktrace and AvePoint

1.2.4 Threat Management

Threat management includes protection from both malicious software and attacks against systems and networks. Microsoft products and services can provide data protection against malware and other types of threats.

Microsoft 365 uses multi-engine antimalware scanning to protect incoming, outgoing, and internal messages from malicious software transferred through email. Administrators can manage antimalware/antispam controls in the Microsoft 365 admin center; individual users can manage their safe senders and blocked senders from within their inboxes in Microsoft Outlook or Microsoft Outlook on the web. Microsoft 365 also includes features that can mitigate the effects of malware attacks, including ransomware attacks.

Microsoft Endpoint Manager includes Intune Endpoint Protection and allows you to set policies to help ensure that computers are kept up to date with the latest antimalware definition updates. Intune can also deliver malware protection to PCs.

Advanced Threat Protection using Defender for Endpoint provides real-time protection from unknown and sophisticated attacks on your Emails, Workstations and AD Domain. It also protects users from unsafe attachments\files and provides real-time, time-of-click protection from malicious links that are included in messages and documents stored in Office 365. Advanced Threat Protection using Defender for Office 365 complements the security features of Exchange Online, Windows Defender, On-premise and cloud environments to help provide better protection from zero-day to unknown attacks.

Threat management typically covers the following products: Microsoft Cloud App Security – security for other SaaS and non-SaaS solutions, Microsoft Defender XDR (Suite of Advanced Threat Protection solutions), Microsoft Endpoint protection, but might also cover third-party solutions such as zScaler, Proofpoint, Sophos, Darktrace, Cybereason, SentinelOne, AT&T and Qualys.

1.2.5 Windows Client

Windows Enterprise can provide the following enhanced security features to mitigate against security breaches and attacks.

- Defender Anti-Virus
- Defender for Endpoint
- Defender SmartScreen
- Defender Application Guard
- Defender Application Control
- Defender Exploit Guard
- Defender Credential Guard
- Windows Firewall
- Windows Hello for Business
- Windows Information Protection

1.3 Benefits

This service will provide the following business benefits:

- Security deployed directly into you Microsoft 365 tenant
- Walkthrough of implemented security features.
- Documented deployment

1.4 Timescales

This Service is typically a various length engagement which is dependent on the scale and size of your organisation, the amount of data/content involved and your starting point.

1.5 Pricing

All Pricing is in accordance with the SFIA Rate Card attached to the Service definition entry on the digital marketplace portal.

1.6 Terms and Conditions

Terms and conditions are in accordance with the G-Cloud 15 Framework agreement and call off contract.

1.7 Invoicing Process

- All work is proposed and delivered using ElysianIT terms of business.
- ElysianITs' Payment terms are 30 days' net from date of invoice, Payment of invoices will be made in Sterling.
- All financial queries and correspondence to ElysianIT: finance@elysianit.com
- The registered address of ElysianIT Ltd is: Upper Farm, Wootton St. Lawrence, Basingstoke, Hampshire, RG23 8PE

1.8 Customer Responsibility

In each engagement there will be a range of dependencies on the customer which are specific to each project. These will be discussed and agreed prior to commencement and will form part of the contract.

2. Why ElysianIT – *making IT effortless*

ElysianIT are a Microsoft Solutions Partner, established in 2014.

We provide professional services/consulting and Managed Support with staff that have extensive experience of Microsoft on-premise and cloud services, working with Microsoft 365, Azure, Active Directory, Windows server and desktop clients and Enterprise Mobility and Security (EMS), alongside the second-generation cloud products that are now reaching maturity, including elements such as the Power Platform and Azure PaaS services.

We pride ourselves in building partnerships with our clients to identify targeted changes to technologies which provide the business with multiple benefits.

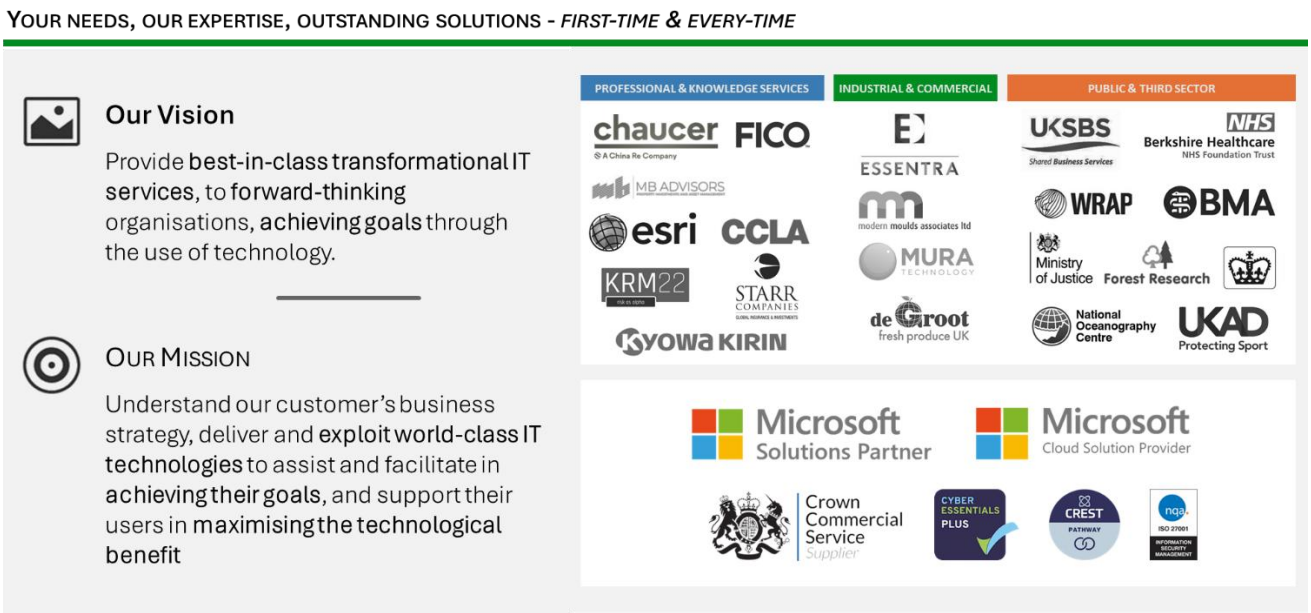
These include the end user experience of IT, increased productivity and security, and/or reduced overall costs.

With our long-term heritage, working with public sector and private organisations we have developed a series of security baselines and processes inline with NCSC Guidance, CIS Benchmark and Microsoft Best Practices which we use to accelerate the design and build phases.

These are known as our Zero to Hero security baselines.

We place great emphasis on building effective and trusted partnerships with our clients to identify targeted and considered changes to technologies which provide the business with multiple benefits.

These include the end user experience of IT, increased productivity and security, and/or reduced overall costs.



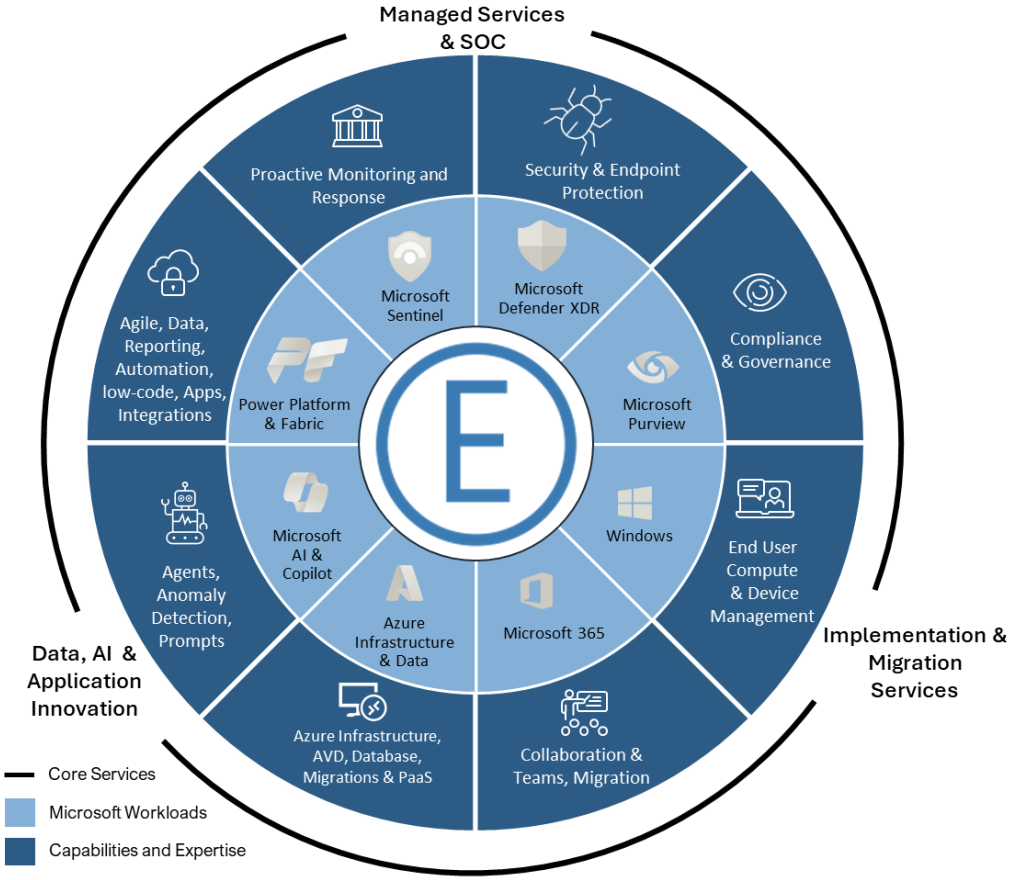
2.1 Our Credentials

The below competencies are aligned to our Microsoft Partner Account on the Solution Providers site.

ElysianIT company registration number is 09245203, established in 2014. DUNS Number: 220402392

2.2 Our Core Services

Offering a range of intelligent business change and implementation services focussed on Microsoft technologies.



2.2.1 Intelligent Advisory – ensuring you're future ready

<u>Technology experts on-demand</u>

Partnering with ElysianIT gives you direct access to our ***Virtual 'C-level' Advisory Services***. Not only ensuring that you're getting the best from your current technology, but our Senior Consultants horizon scan to verify that your technology decisions are both future-proof and strategically aligned with your goals.

We pride ourselves in understanding your organisations strategy to deliver transformative technology with outstanding solutions, moving you from just ***operating to innovating***.

2.3 Our Impact – *trusted by peers*

With experience of working with organisations ranging in size from a handful of users to thousands, we relish solving challenges these organisations bring.

2.3.1 Partnering in focus - *delivering transformational results*

CHARITY COMMISSION FOR ENGLAND AND WALES

The Charity Commission for England and Wales (CCEW) is the non-ministerial government department that regulates registered charities in England and Wales and maintains the Central Register of Charities. CCEW has around 550 users across 4 UK sites.

ElysianIT has delivered the following services and has continued to support the organisation for over 5 years.

- Planning and Design for a full IT estate modernisation comprising Windows 11 roll out, Office 365 onboarding, Enterprise Mobility Suite and migration of on-premise estate to migration
- Design of a modern desktop management approach comprising Intune and Autopilot
- Implementation of a highly secure M365 collaboration environment including Teams, SharePoint, OneDrive for Business and the Office client
- Active Directory audit, recommendations, modernisation & rationalisation
- Identity Management, Conditional Access, MFA and Self Service SPR
- Deployment of a Hybrid Exchange environment and migration of all mailboxes
- Design and build of an Azure landing zone to cater for their hosting requirements and migration of circa 50 servers
- Rebuild all of user devices to Windows10 and implementation of supporting iOS device estate
- Project & Change Management and Governance
- Ongoing 3rd Line Microsoft Azure Cloud Support

UKAD Protecting Sport

UK Anti-Doping (UKAD) is a Non-Departmental Public Body accountable to Parliament. UKAD is the national organisation dedicated to protecting a culture of clean sport in the UK. UKAD have around 100 users across 2 main UK sites.

ElysianIT has delivered the following services and has continued to support the organisation for over 10 yrs.

- Cloud Strategy and Business Case
- Planning and Design for Azure, Microsoft 365
- Change Management and Governance
- Windows 11 Rollout
- Exchange Online Email migration
- Intune for Device Management
- OneDrive and SharePoint Site Migration
- SharePoint Intranet Development
- Data centre replacement into Azure Services
- Web Hosting migration to Azure Services
- PKI Infrastructure
- Azure Sentinel, Monitoring and Intune
- Ongoing Fully Managed Service (Support)

2.4 Microsoft CSP – *Licensing without the hassle*

ElysianIT is a Microsoft Cloud Solution Provide (CSP) and therefore can transact Azure cloud service costs directly with our customers.

The Cloud Solution Provider (CSP) Program enables purchases of Microsoft online service subscriptions (M365), Azure services, and some on-premises software via the Microsoft Customer Agreement.

The CSP allows you to take advantage of True PAYG billing and benefit from the highest discounts through Reserved Instances, Hybrid Benefits and Software Subscriptions.

2.5 Getting in Touch – *share your thoughts*

We work on a no-obligation basis and welcome the opportunity to discuss how we can help organisations realise business change and the associated benefits through the application of technology.

UK Office – Basingstoke

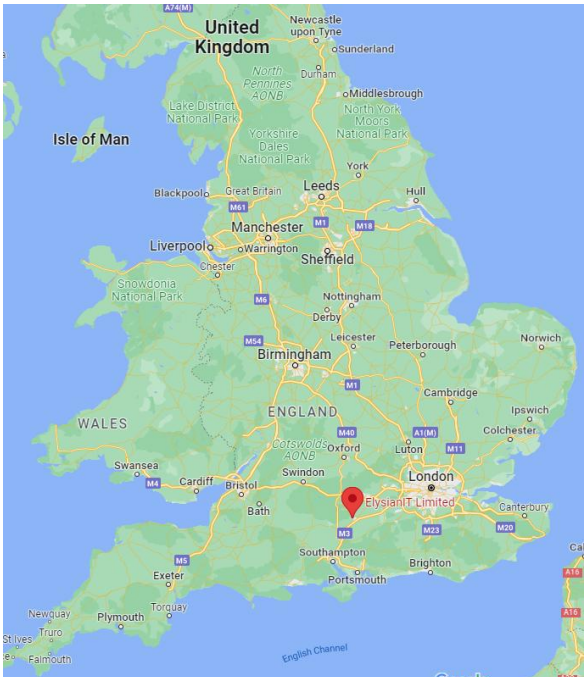
ElysianIT Ltd
Upper Farm,
Wootton St. Lawrence,
Basingstoke,
Hampshire,
RG23 8PE

www.elysianit.com

01256 976 650

info@elysianit.com

Follow us



3. Methodology and Approach – *turning ideas into value*

ElysianIT embrace a consultative approach to each project engagement, taking time to understand the key challenges, then leveraging our expertise and combined knowledge of the technology capabilities to address the business challenge(s) and achieve your goals.

We align specific resources throughout the engagement phases to ensure smooth running, alignment of shared values, effective communications, and management with the goal to ensure that we expedite projects efficiently.

•**Account Manager**– has full authority to make decision with regards to the commercial and contractual elements on behalf of Elysian IT. Responsible for the client relationship.

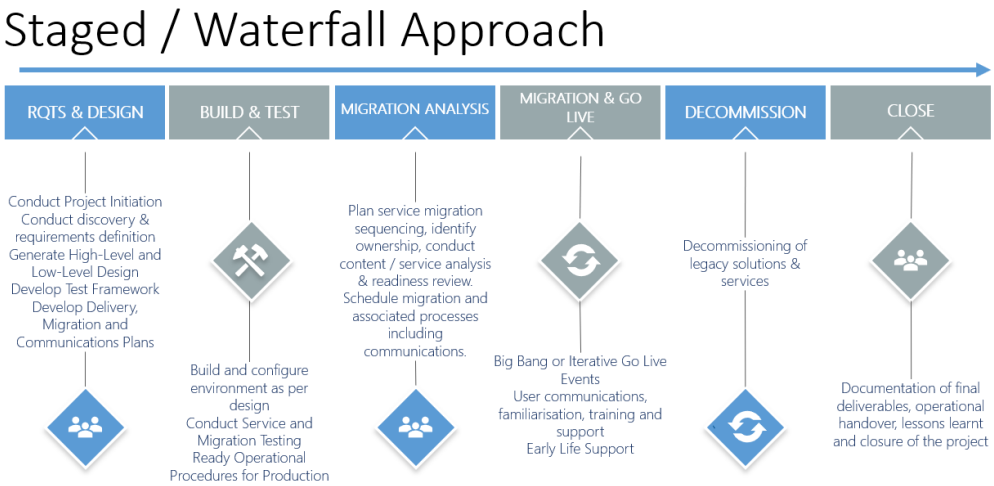
•**Technical Account Manager** –Responsible for having a holistic view of the operational technology and processes within a given account.

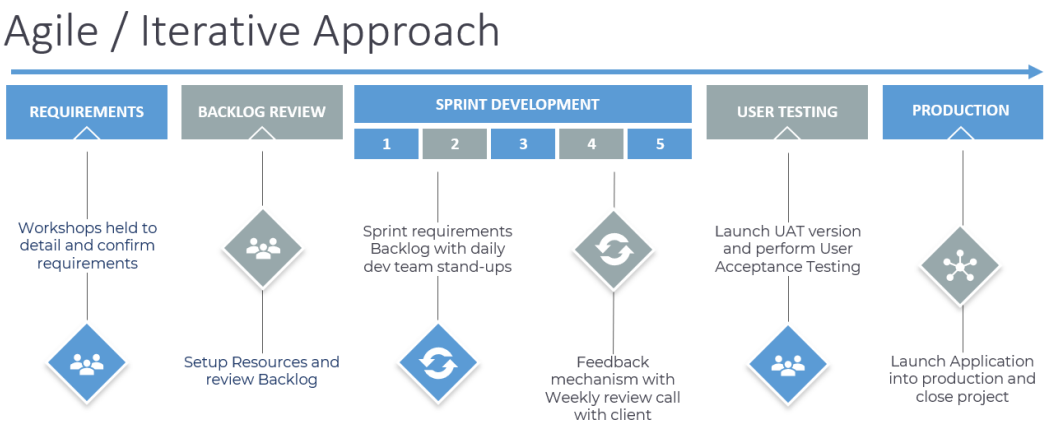
•**Service Management** – Responsible for the day to day running of the Managed Service / Support and ensuring that standard monitoring activities are conducted, that ticket and issues raised are resolved in line with the agreed SLA, that reports are generated on the agreed schedule and that quarterly reviews are scheduled and conducted.

•**Project Management** – for discrete project delivery aspects, a dedicated Project Manager will be provided to work with client resources to plan and coordinate the work of the required technical resources.

Our engagement methodology is often determined by a client's current operating model, or our role within an overarching project – we are conversant with many different approaches and have qualified, experienced project managers who assist with integrating into your required processes.

We typically use a simple yet effective & scalable traditional waterfall style management structure for infrastructure or migration engagements and an agile style, where appropriate, for our software development projects.





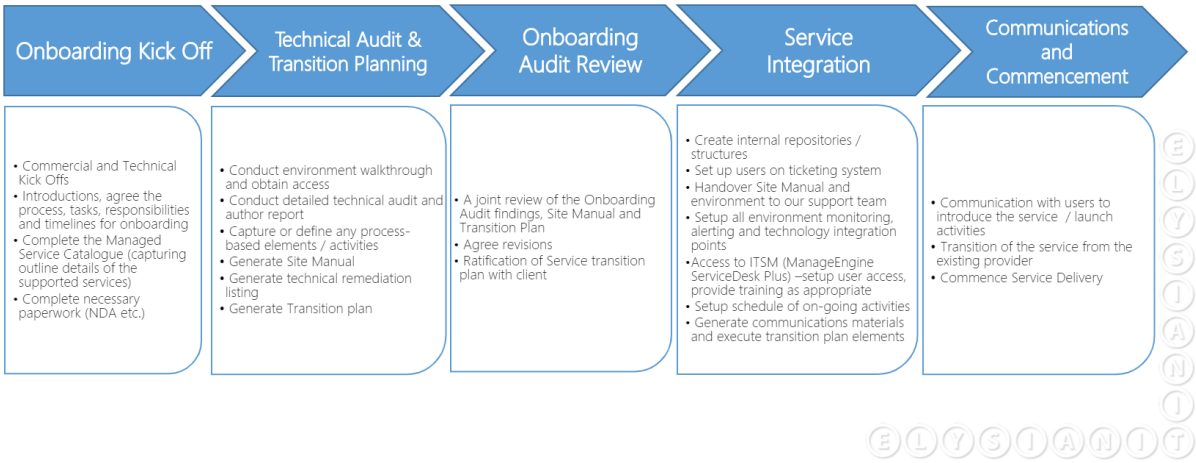
ElysianIT has, over the course of hundreds of successful engagements, adopted these methodologies to enable our consultants to focus on collaboration with our clients in long-term partnerships, ensuring full transparency and that everyone has common understanding on the agreed expectations.

4. Support and Training – *expertise on-tap*

Every Service engagement we deliver will be backed up by our support team with numerous options for how this support can be delivered. In addition, we have Microsoft Certified Trainer embedded experience in house, which provides key Transition and Adoption activities to assist with the delivery of end-user, expert or administrator focussed training and business change activities with the appropriate supporting collateral.

Our support team members all have at least 5 years commercial experience, and we ensure that every member of the team is trained across the broad concepts of Microsoft 365, EMS and Microsoft Azure and undertake the relevant Microsoft Certifications (MCPs). Ensuring that we maintain skilled and experienced staff, with the necessary qualifications and experience, to achieve the right outcomes.

The support onboarding and handover process are engaged in advance of the project delivery completing this ensures our clients and our Support Team understand the scope of support whilst tracking and triaging early adopters or migrated end users' requests in a controlled fashion and to ensure that the transition to support is smoothed through the conclusion of the delivery project.



Every Support client has access to the following facilities:

- Dedicated Email address
  - Automatically creates a ticket in the Service Desk software when received
- Dedicated telephone number
  - Staffed by UK based support individuals, not outsourced
- Online Service Desk
  - Implemented with Single Sign On (SSO) for users of Microsoft 365 - Azure AD
  - Users can raise issues and request tickets with appropriate SLAs
  - Allows users to monitor issue progress and update issue information 24/7
  - Provides links to FAQs and help guides
  - Provides a survey to users subsequent to ticket closure to garner feedback on their experience and drive service improvement

- Our Service Desk system is configured to effectively manage issue resolution and management to agreed SLAs. Tickets nearing SLAs automatically alert the ElysianIT ticket owner and management team to ensure quality and timeliness of delivery

Issue Management and Resolution to SLAs - Once any issue is raised it is proactively managed through its lifecycle. A Priority level is assigned, and an appropriate response initiated. Priority 1 issues are alerted to the management team to ensure any resources required are mobilised to provide the quickest path to

resolution. All other tickets are acted upon according to priority and the associated SLA response and resolution times.

Security impact - All issues/requests raised are evaluated against security for validity and impact. Any request for elevation/changes in access are always verified via the user's line manager for authorisation prior to execution. Any change requested is reviewed against the defined security principals.

Service impact – Considering the impact to service of any change requested is a fundamental part of the issue triage process to assess any threat and maintain security whilst supporting the user to achieve the desired resolution. All ElysianIT Service Desk resources are suitability trained on both the core technologies and the specific customer procedures to ensure that they both understand and consider the impact of any actions they take.

Continual Service improvement - to ensure continual service improvement ElysianIT undertake the following activities:

- Weekly senior team review of all tickets – Open/In-progress/Closed (during week), appropriate actions are undertaken/scheduled to ensure quality of service and to ensure no SLA breeches. Tickets details, issue handling, recurring related incidents and resolution are reviewed. The review will highlight the need for updating the FAQs, publishing a help guide or IT remediation activity (e.g. hotfix update or general improvements etc). Any underlying problems or security concerns are raised directly to yourselves where we will jointly address root cause analysis

- Support ticket reports are reviewed, and trends/issues/service improvement activities are added to the scheduled Quarterly Customer Review meeting agenda. This ensures that support issues are discussed and addressed on a regular ongoing basis (providing a rhythm to the service)

- ElysianIT maintains an IT Operations Guide that provides detail of the procedures/configurations/processes for the IT environment. The weekly support ticket review ensures updates and augmentation to this guide are undertaken in a timely fashion

- Best practice, security, process and control are underpinned by the weekly reviews to ensure quality of service, cross team learning and experiences from other clients are integrated into the service that you receive.

- ElysianIT is a Microsoft Gold partner and invest heavily in staff training to ensure that they are well versed in the latest technology and updates in the marketplace, ensuring that our clients can benefit from the experience.

On-site support is an available service. It is important that the onsite support staff are both technically competent and interact with our client's users an appropriate fashion. During the weekly support ticket review onsite support issues are discussed and these on-site learnings are fed into the continual improvement process to update procedures/practices.