Elysian:IT

Microsoft Solutions Partner

CYBER ESSENTIALS PLUS

nqa ISO 27001 INFORMATION SECURITY MANAGEMENT

G-Cloud 15

Managed SOC Service

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*

The ElysianIT *Managed Security Service* is a managed Security Operations Centre (SOC) service underpinned by our SIEM and SOAR solution Microsoft Sentinel and the Microsoft Defender XDR suite. It delivers Managed Detection and Response (MDR) capabilities, combining automation, expert triage, and human-led incident response to protect your digital estate.

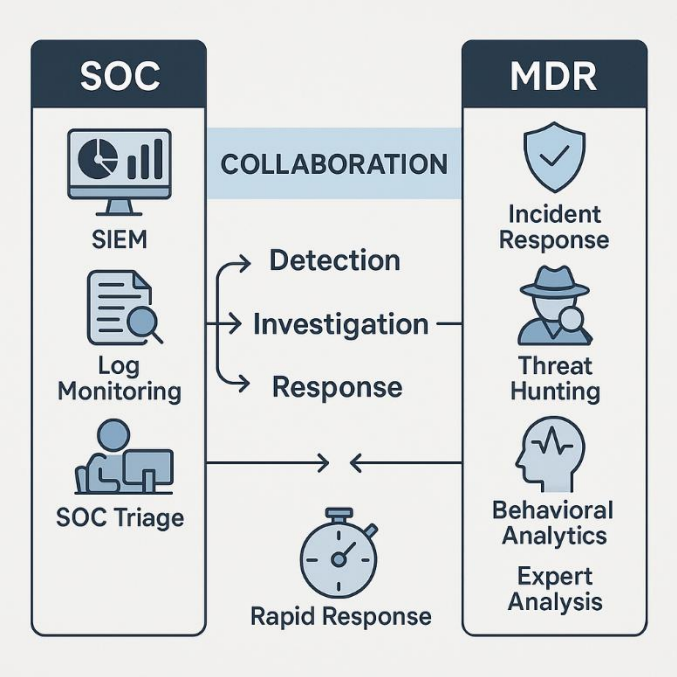


Figure 1 - Managed Security Service Overview

1.1 What is a SOC

At ElysianIT, our Security Operations Centre (SOC) forms the foundation of our cybersecurity services, delivering 24/7 monitoring, SIEM, SOAR, log analysis, and SOC triage to detect and assess potential threats in real time.

Closely integrated with our Managed Detection and Response (MDR) service, the SOC acts as the first line of defence—identifying suspicious activity and escalating validated threats to our MDR team for rapid investigation and containment. This synergy ensures a streamlined, end-to-end response process, where alerts are not only detected and triaged efficiently but also acted upon with expert precision.

Together, our SOC and MDR services provide customers with a unified, adaptive security posture that protects against both known and emerging threats.

1.2 What is MDR

The ElysianIT Managed Detection and Response (MDR) service is tightly integrated with our in-house Security Operations Center (SOC) to deliver a seamless, end-to-end cybersecurity solution.

While our SOC provides 24/7 monitoring, log analysis, and triage of security events, our MDR team takes it further—leveraging advanced analytics, threat intelligence, and expert-led investigations to proactively hunt for threats and respond to incidents in real time.

This collaboration ensures that every alert is not only detected and triaged quickly but also escalated and contained with precision and by combining the strengths of our SOC and MDR, we offer our customers a unified, agile defence that adapts to the evolving threat landscape and minimises business risk.

1.3 How it works

Our Manager Security Service leverages existing CCEW technologies, including Sentinel and the M365 Defender Suite, to enhance threat detection and monitoring.

Our approach includes customising alerting rules to minimise false positives and evolving the security tooling to improve the security posture and automated containment for swift incident response.

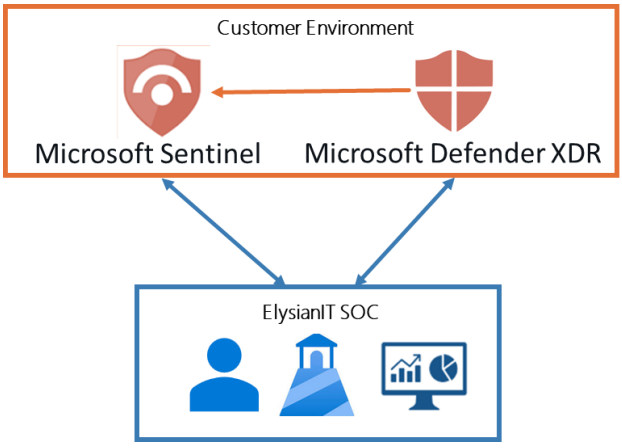


Figure 2 - ElysianIT Managed Security Service

Additionally, we provide comprehensive cyber incident reporting and collaborate closely with CCEW's internal resources, ensuring a seamless enhancement of your security posture. In this model, all security data stays under CCEW's tenancy and control.

1.4 Capabilities

ElysianIT Managed Security Service Capabilities are:

- **Monitoring & Detection**: monitoring of telemetry from Microsoft Sentinel and Defender to detect threats.
- **UK Manned SOC**: ElysianIT only employ UK Staff which are at minimum BPSS Cleared.
- **Triage & Escalation**: All alerts are triaged by SOC analysts and confirmed incidents are escalated either to the customer's internal team for deeper analysis or to the ElysianIT Incident Responders or Security Consultants for containment.
- **Incident Response**: ElysianIT provides containment actions (e.g. host isolation, credential revocation) based on pre-agreed rules of engagement.
- **Security Reporting**: Security reporting with executive summaries, incident metrics, and recommendations for posture improvement.
- **Incident Response Remediation Support**: Optional block hours for proactive remediation, configuration hardening, and policy tuning.

1.5 Service Features

ElysianIT Managed Security Services offer a robust managed detection and response service for small, medium, and large organisations.

Our service is built on top of the Gartner* leading Microsoft Sentinel and Defender XDR (Cloud & M365) suite of products, and each service is inclusive of the following key components (aligned to the Clients Microsoft licensing).

Anything outside of this scope is not covered by ElysianIT's Managed security managed service (including 3rd party products and services – unless specified in the Managed service add-ons)

The following table lists the features and items which are in and out of scope:

Features	In Scope	Out of Scope
Service Onboarding	✓	
UK business 08:00-16:00 SOC Service	✓	
UK business 24x7 SOC Service		✓
Email Address and Phone number	✓	
Responsive SLAs	✓	
24x7 Microsoft Sentinel Monitoring	✓	
Automated Containment (device isolation)	✓	
ElysianIT Support Service Portal	✓	
Security Reporting & Meeting	✓ - Monthly	
Strategy Reporting & Meeting	✓ - Quarterly	
Investigation for M365/Sentinel security alerts	✓	
Security alert containment (connected Sentinel data sources)	✓	
Microsoft XDR Complete Threat coverage **	✓ - where licensed and configured	
System Improvement hours (Days) ①	✓ 48 (6) + procure additional time	
Incident Response hours (Days) ①	✓ 48 (6) + procure additional time	
Proactive Threat Hunting **		✓
Managed – Endpoint, Detection & Response (Microsoft Defender for Endpoint)		
Endpoint Protection ②	✓	
Conditional Access	✓	
Device Compliance	✓	
Threat Analytics**		✓

Features	In Scope	Out of Scope
Web Content Filtering	✓	
Attack Surface Reduction* ***(Initial Audit Mode 30 days – then transfer to Block mode)*** ③	✓	
Vulnerability Alerting ④	✓	
Vulnerability Patching ④		✓
Managed – Cloud Protection (Microsoft Defender for Cloud)		
Cloud workload protection core – includes		
Cloud Security Posture Management (Foundational)		✓
Defender for Cloud workload protection (Servers)	✓ ⑤	
Defender for Cloud workload protection (Databases)	✓ ⑥	
Defender for Cloud workload protection (Containers)	✓	
Defender for Cloud workload protection (Storage)	✓	
Defender for Cloud workload protection (Service Layer)	✓	
Cloud workload protection advanced – In addition to the above, also includes		
Cloud Security Posture Management (Advanced)		✓
File integrity monitoring		
Just in time access scanning		
Container Image scanning		
Adaptive Application Control		
Adaptive Network Hardening		
SQL Vulnerability Management		
Email and Collaboration (Defender for Office 365)		
Anti-Phishing	✓	
Real Time Detection*	✓	
Safe Attachments*	✓	
Safe Links*	✓	
Anti-Malware	✓	
Simulated Phishing Attacks*		✓
Attack Simulation Training for Client*		✓
Cloud Applications (Defender for Cloud Apps)		✓
Discovered Apps*		✓

Features	In Scope	Out of Scope
Cloud App Risk Assessment **		✓
Anomaly Detection for Discovered Apps **		✓
App Permissions and Ability to Revoke Access **		✓
Real-time Session Monitoring and Control **		✓
Identity Protection (Microsoft Entra ID Identity Protection)		
Identify Anonymous IP Address Use **	✓	
Atypical Travel **	✓	
Malware Linked IP Address **	✓	
Unfamiliar Sign-in Properties **	✓	
Leaked Credentials **	✓	
Defender for Identity (for hybrid AD signals)		
Monitor users, entity behaviour, and activities **	✓	
Protect user identities and credentials stored in Active Directory **	✓	
Identify and investigate suspicious user activities **	✓	
Microsoft Defender for External Threats		
External Attack Service Monitoring **		✓
Managed Microsoft Sentinel		
Sentinel Deployment, configuration, and integration (Including Azure Lighthouse setup and configuration)	✓	
Microsoft (out of the box) connector setup	✓	
Monthly Sentinel cost reporting & optimisation		✓
Additional Sentinel (3rd party) connectors ⑦		✓
Custom Connector integration ⑦	✓ - 6x Cisco Meraki Firewalls only	✓ - Other than Cisco Meraki
Threat Hunting **		✓
Threat intelligence **		✓
Managed Incident, Detection and Response ⑧	✓	
Other		
Implement Security baselines	✓ (using System Improvement hours)	
Participate in incident response tabletop exercise **		✓
Behavioural Analytics		✓

*https://www.microsoft.com/en-us/security/business/reports-analysis/industry-recognized-cybersecurity-leader
** Microsoft 365 E5 Security Add-on

Note

1. Pre-allocated time blocks for in-depth investigation, root cause analysis, and remediation of escalated incidents. Used for high-priority or complex cases, with defined SLAs. more hours can be purchased upfront as part of service contract at discounted rate
2. Endpoint Protection is limited to 600 Windows Devices which are onboarded into Defender for Endpoint Protection
3. Security Engineering time dedicated to implementing enhancements, optimisations, and new features. Activities include fine-tuning alert rules, integrating new tools, and improving detection logic. Time will be pre-organised and can be used out-of-hours where enough notice has been given. more hours can be purchased upfront as part of service contract at discounted rate
4. Vulnerability management core (as a part of Microsoft Defender for Endpoint Plan 2) includes device discovery, device inventory, vulnerability assessment, configuration assessment, risk-based prioritisation, remediation tracking, continuous monitoring and software inventory/usage (Vulnerability Management details)
5. Coverage for 150 server instances (Defender for servers) included as part of service – additional servers will be charged accordingly
6. Coverage for 5 database instances (Defender for database) included as part of service – additional servers will be charged accordingly
7. Limited to point 2 additional connectors can be added, but will be charged separately
8. Limited to detect & alert and automated response.

1.6 Service Level Agreement (SLA)

The following table details the service level agreement:

Alert Level Priority	Description	Cyber Security Response Times
Alert Acknowledgement	An alert was raised and a ticket logged in Zoho ServiceDesk Plus via Sentinel Alert Rule. The ticket was acknowledged, but no action or triage has occurred; the client was notified that the incident is being addressed.	The SOC team will acknowledge within 15 minutes
Critical (P1)	Mission critical, business impacting incident	The SOC team will respond within 15 minutes
High (P2)	High impact to client systems, such as data leakage, malware infection	The SOC team will respond within 1 hour
Medium (P3)	This is a medium impact to client systems	The SOC team will respond within 4 hours

Low (P4)	Little impact to client systems	The SOC team will respond within 24 hours
Informational (P5)	No impact to client systems	The SOC team will respond within 48 hours
Change / Service Improvement (P6)	No impact, new service implementation or changes	Best endeavours

The security alerts are triaged before being assigned to an incident responder. A security alert is a raised ticket via a Sentinel Incident.

Tickets are assigned a priority based on the sentinel alert priority, which will be used on that ticket, thus resulting in the required response and resolution time.

Timer starts when the ticket is received and stops when the responsibility is back with the customer or with a 3rd party. The timer starts again as the ticket is passed back to ElysianIT.

Change / Service improvements are subject to the Change Request Management definition in section **Error! Reference source not found.**.

1.6.1 Determining Incident Severity

Incident severity levels are classified by Microsoft Sentinel or Defender XDR.

1.6.2 Incident Severity Evaluation

While initial Incident Severity and the Asset Criticality are pre-determined, Initial Incident Likelihood is determined only through investigation.

This investigation includes evaluating context and conducting analysis. In all cases, ElysianIT Security Operations Centre SOC Analysts set the Incident Severity based on all available input, layered with their expert judgement.

1.6.3 Incident Response Process

The following diagram provides an example of a P1 Response process

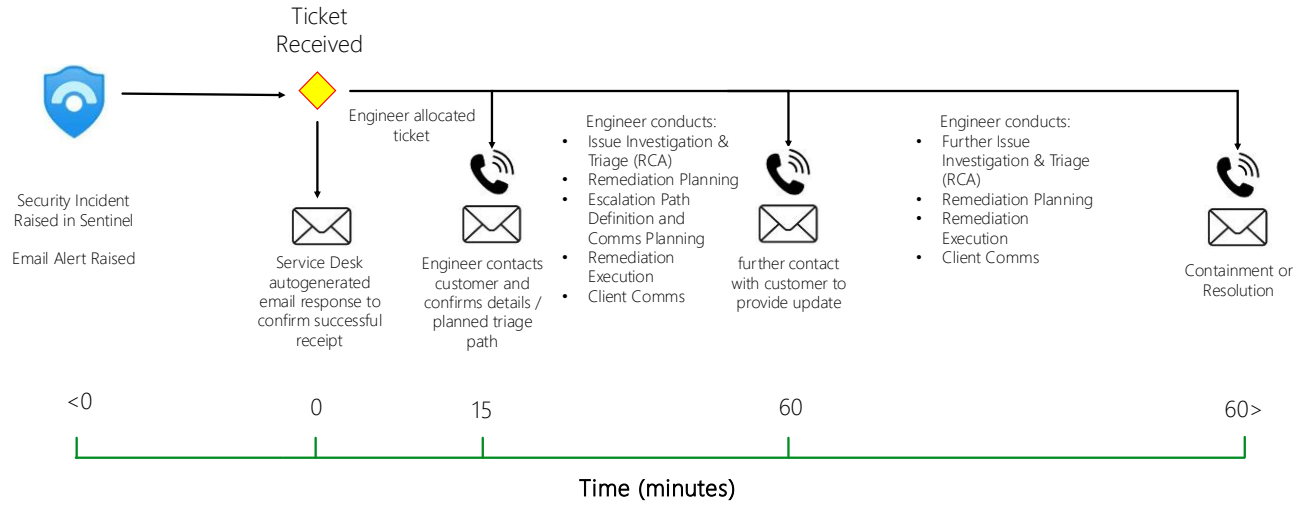


Figure 3 - Incident Response Process Example

1.7 Benefits

ElysianIT Managed Security Service provides the following benefits:

- **Expertise and Resources -** Access to a team of security experts with extensive experience in managing and responding to security incidents across various environments.
- **Cost-Effective Solution -** Reduces the need for dedicated in-house security resources, allowing your organisation to focus on core business activities while we manage your security needs.
- **Scalability -** Our MDR service is designed to grow with your business, easily adapting to changes in your cloud infrastructure and security requirements.
- **Peace of Mind -** With ElysianIT managing your security operations, you can focus on innovation and growth, knowing that your digital assets are protected.

1.8 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.

1.9 Pricing

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

1.10 Terms and Conditions

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

1.11 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

1.12 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.

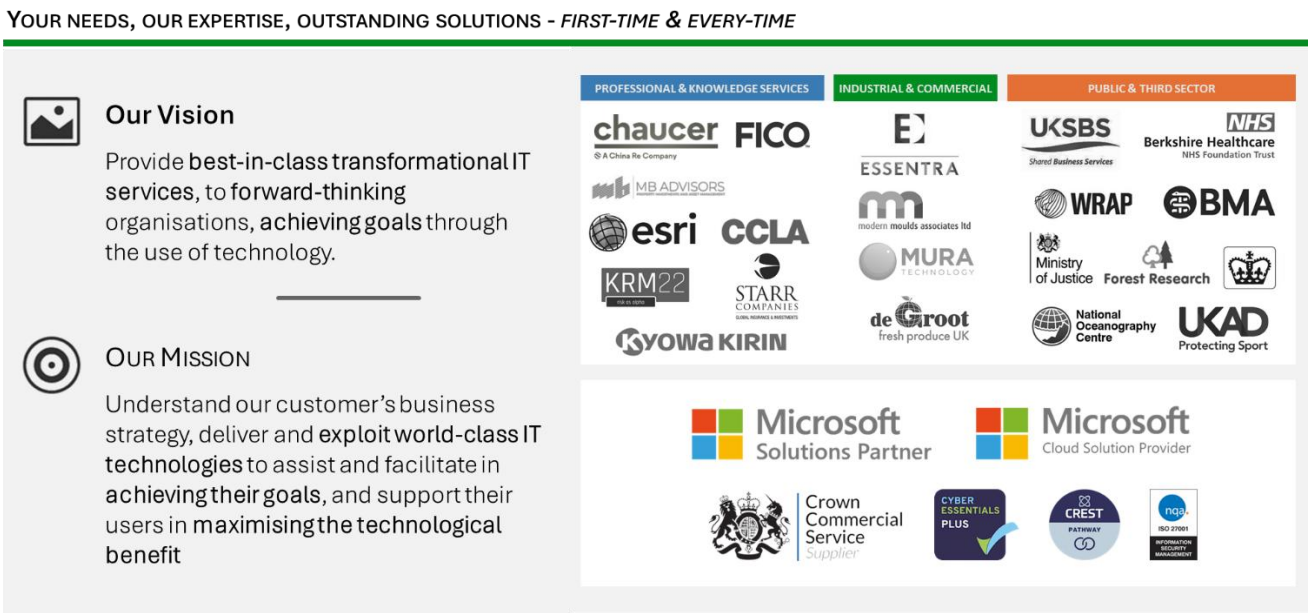
These include the end user experience of IT, increased productivity and security, and/or reduced overall costs.

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.



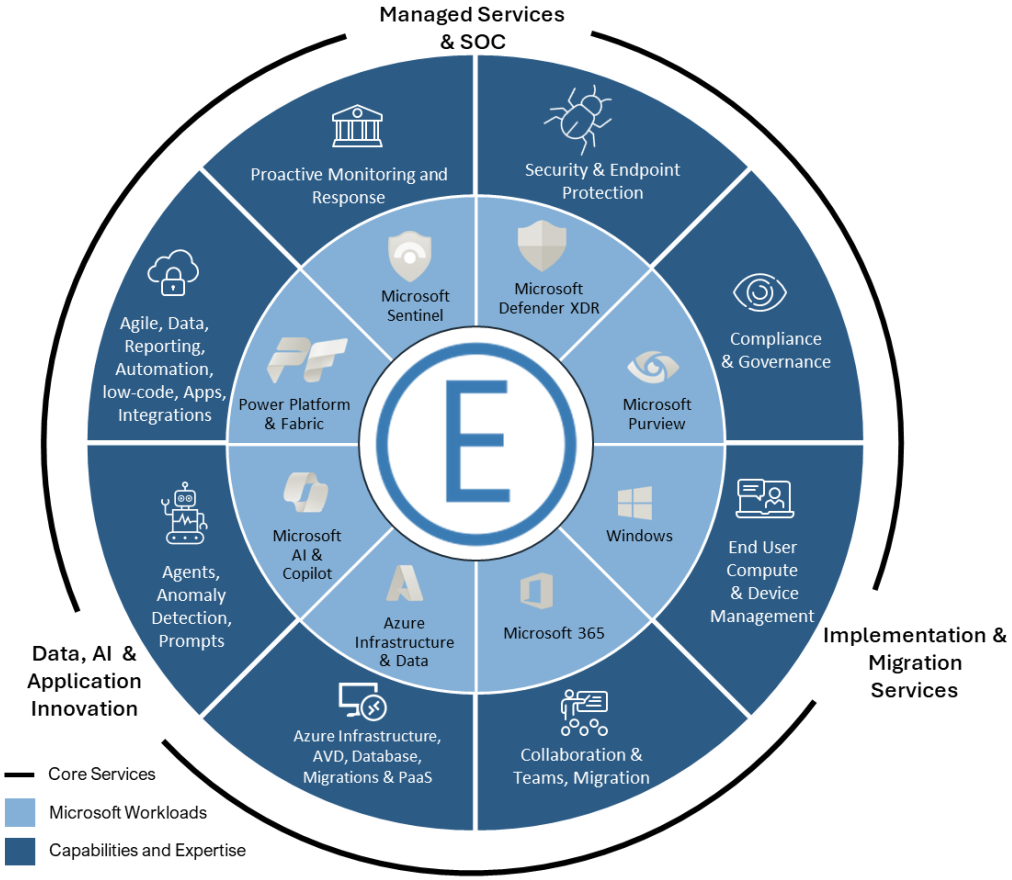
2.1 Our Credentials

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

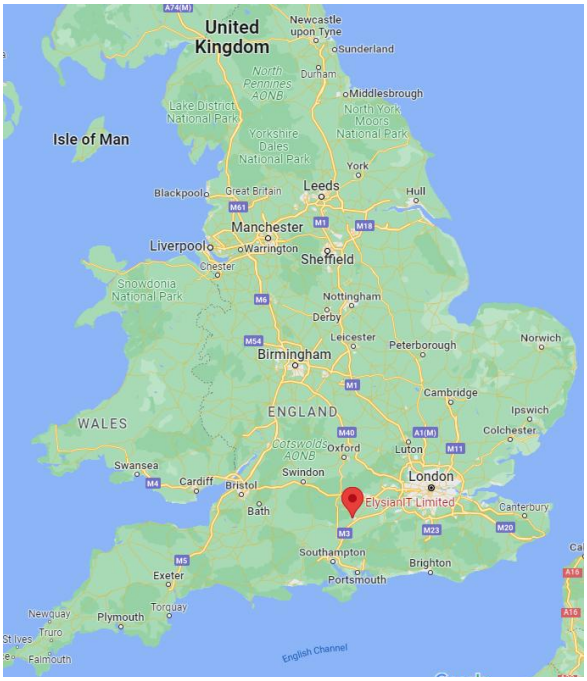
ElysianIT Ltd
Upper Farm,
Wootton St. Lawrence,
Basingstoke,
Hampshire,
RG23 8PE

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.

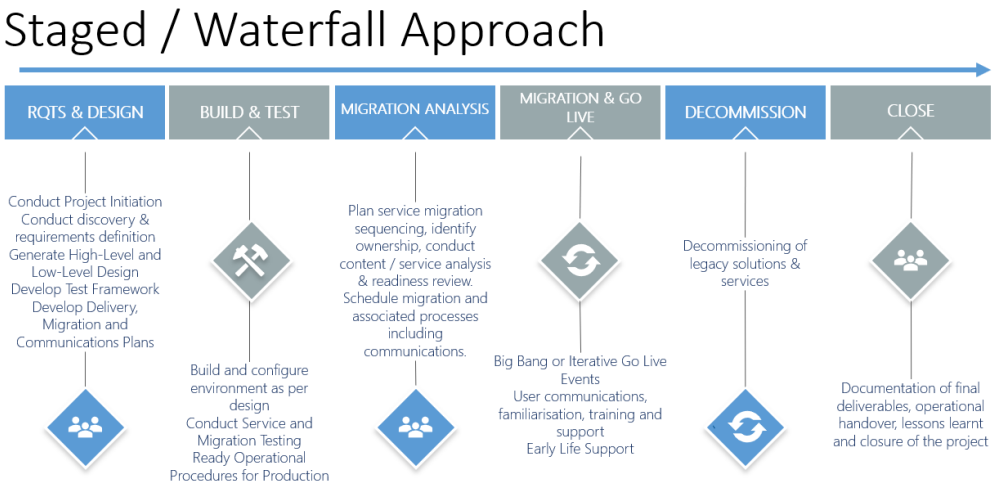
•**Technical Account Manager** –Responsible for having a holistic view of the operational technology and processes within a given account.

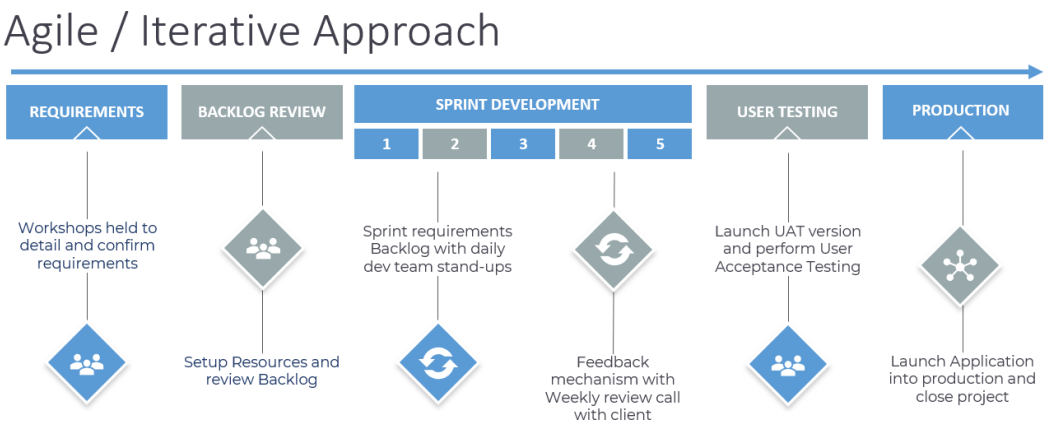
•**Service Management** – Responsible for the day to day running of the Managed Service / Support and ensuring that standard monitoring activities are conducted, that ticket and issues raised are resolved in line with the agreed SLA, that reports are generated on the agreed schedule and that quarterly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





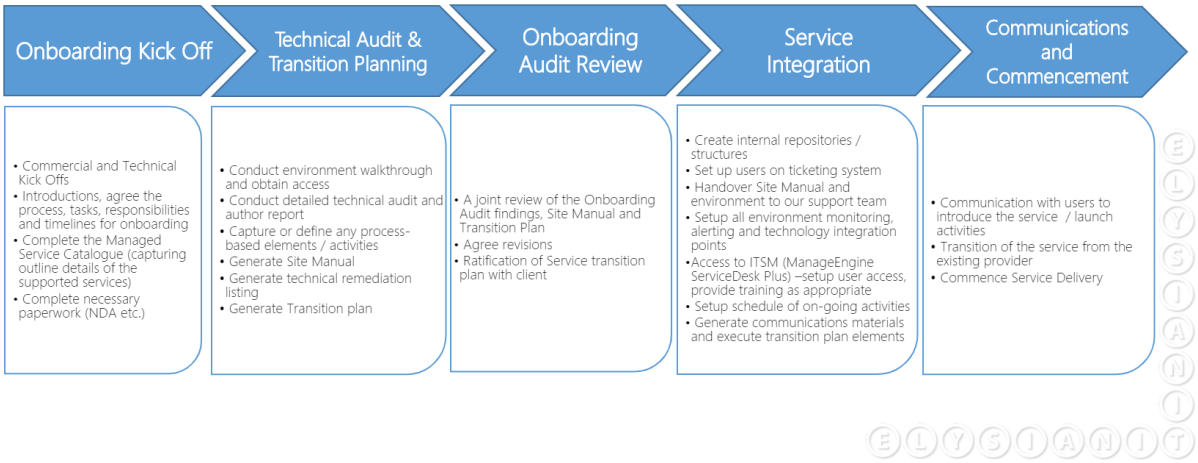
ElysianIT has, over the course of hundreds of successful engagements, adopted these methodologies to enable our consultants to focus on collaboration with our clients in long-term partnerships, ensuring full transparency and that everyone has common understanding on the agreed expectations.

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.