G-Cloud 15
Service Definition

Aspire Penetration Testing Services

Aspire Technology Solutions

Table of Contents

Introduction

Company Overview

Aspire Technology Solutions is an award-winning IT Managed Service Provider and Internet Service Provider. We deliver leading technology solutions across cloud, connectivity, telephony, technical support, cyber security, and professional services to help our customers drive real organisational benefits.

Our mission is to deliver technology like no other; we are dedicated to putting technology to work to help our customers innovate, become more efficient and grow quicker.

We have an extensive customer base across the UK including SMEs, public sector, and not-for-profit organisations as well as large enterprises and blue-chip organisations with a global presence. We provide services across multiple sectors, to a vastly diverse portfolio of organisations, which means our experience is well-rounded and our expertise is constantly tested to the highest levels.

We help our customers accelerate their ambitions through inspirational technology and to achieve this, we have a passion for delivering a sensational data-driven customer experience. To make sure we're on track, we measure our performance using the Net Promoter Score (NPS) global measure. In the past 12 months our score has averages +82 which is deemed 'world-class'.

At Aspire, we design and deliver innovative IT solutions that drive organisations forward. In a world that's changing faster than ever, we expect our customers to expect more from their technology.

Value Proposition

As a managed security service provider with extensive experience in providing both cyber and information security services, we understand the security challenges and requirements facing organisations. We believe that we are an extremely suitable IT security service partner who can provide the managed security services you require today, but we are also dedicated to working with you to provide the IT service flexibility to develop the way your services will be delivered in the future.

Our value is demonstrated through the technology journey on which we take our customers. At Aspire, our mission is to deliver technology like no other; we are dedicated to putting technology to work to help our customers innovate, become more efficient and grow quicker. Through our dedicated account management, we will form a deep understanding of your organisation, your challenges, and your opportunities. We then use our vast experience of technology and industry trends to develop a roadmap aligned to your organisational strategy to ensure that all services provide real value.

We will work hard to build a robust and mutually beneficial relationship with you, supporting your network, infrastructure, applications, and systems to maximise opportunities for growth. We are well-versed in providing innovative IT security solutions that work. We have designed a service that we know will enhance your cyber security and drive significant value, while minimising risk and striving to reduce cost wherever possible. As part of our commitment to

you, we will assess your security technology spend, identifying and reducing any excessive areas and we will look to deliver improvements using these cost savings.

We believe Aspire have a unique proposition with our data-driven 24/7 dedicated Security Operations Centre (SOC), as well as our separate Network Operation Centre (NOC) helpdesk support offering. Our service delivery methodology, closely modelled on ITIL has been 10 years in the making; this incremental improvement with careful customer feedback at every stage along the way has led us to our current position with record positive feedback and over 99% SLA being met for over 12 consecutive months.

Our level of commitment to customer service is best illustrated by our high customer retention and fantastic Net Promotor Score (82+ which is deemed world class), we would be delighted to introduce you to customers who will verify our claims and explain in their own words, the value we add to their organisation.

Aspire are committed to delivering success to your organisation. With all of the above, we hope to make evident our dedication to working with you as your preferred technology partner.

What This Service Provides

Aspire have partnered with Punk Security to deliver CREST-accredited penetration testing. These tests are designed to improve your organisations cybersecurity posture by identifying and addressing vulnerabilities and weaknesses in your infrastructure before malicious actors can exploit them. In an era where digital threats evolve rapidly, proactive security measures are crucial to safeguarding sensitive data, maintaining regulatory compliance, and preserving business continuity.

By leveraging best-in-class tools and utilising industry frameworks we ensure the highest quality and precision in our Penetration Testing services. Moreover, our approach aligns with the Penetration Testing Execution Standard (PTES) framework, a globally recognised and respected set of guidelines. Following the PTES framework allows us to conduct ethical hacking in a systematic and organised manner, covering every aspect of your cyber-landscape.

Key features of this service include:

- **Real-World Attack Simulation:** Simulate genuine cyberattacks to uncover hidden vulnerabilities before threat actors do.
- **Tailored Testing Methodologies:** Receive assessments designed around your specific infrastructure, applications, and business objectives.
- **Detailed Risk-Based Reporting:** Get prioritised, east-to-understand reports that highlight exploitable risks and actionable remediation steps.
- **Compliance-Ready Assessments:** Support your regulatory and industry compliance needs with rigorous, standards-aligned testing.
- **Reputation & Trust Safeguarding:** Benefit from post-test debriefs, strategic advice, and continuous support for long-term resilience.
- **Delivered by CREST-Accredited Specialists:** Delivered through our trusted partner, Punk Security, a CREST-accredited penetration testing provider, ensuring industry-recognised quality and integrity.

Overview of the G-Cloud Service

The scope of our Penetration Testing services is defined during a call between you, the client, and the tester, Punk Security. Following your assessment, you will receive a detailed report of our findings.

The following service details are just a guideline. Full scope of penetration test and required days can be discussed with your account manager.

Infrastructure Assessment

The following table outlines expected service components of your infrastructure assessment:

Service Component	Description
Pre-Assessment Planning	Prior to testing, we work closely with you to define the scope of your infrastructure assessment including: • In-scope assets (Ips, domains, credentials). • Forbidden testing methods. • Testing schedule. • Communication protocols during testing. You'll have direct access to our penetration testers throughout the engagement.
Internal Assessment	We will simulate an attacker with access to your internal network, either via compromised devices or physical access. This may include: • Exploitation of compromised users and machines via social engineering (e.g. phishing). • Attacker access through physical connection or unsecured wireless networks. • Risks posed by malicious insiders.
External Assessment	We will examine your internet-facing infrastructure to identify exposed services and vulnerabilities that could serve as entry points for attackers. Activities may include: • Full TCP and top UDP port scanning. • Service enumeration and version identification. • Detection of misconfigurations and known vulnerabilities. • Evaluation of intrusion detection/prevention system effectiveness (if required). • Identification of most probable external entry points.

Credential Scanning	We'll run credentialed vulnerability scans using provided credentials to uncover deeper, potentially long-term vulnerabilities that unauthenticated scans may miss.

Add-on Services

There are several optional services that can be added to the scope of your infrastructure assessment including:

There are several optional services that can be added to the scope of your infrastructure assessment including:

Firewall Review – We'll carry out an assessment of your firewall configurations for unnecessary risk and highlight opportunities for improvement.

WiFi Review – A WiFi review is included in all on-site assessments, or as an additional option for remote assessments.

Attack Surface Assessment – We'll review your infrastructure's Attack Surface, highlighting any potential risks or weaknesses that may be exploited by a threat actor.

Web Application Assessment

The following table outlines expected service components of your Web Application assessment:

Service Component	Description
Web Application Assessment Overview	Prior to testing, we work closely with you to define the scope of your Web Application Assessment.
Core Vulnerability Assessment	We will assess the application against a range of common and critical weaknesses, including: • Injection flaws. • Authentication weaknesses. • Poor session management. • Broken access controls. • Security misconfigurations. • Database interaction errors. • Input validation issues. • Application logic flaws.
Source Code Review	If access is available, we will conduct a secure code review to identify vulnerable coding practices, logic flaws, insecure dependencies, and unsafe functions that may not be visible through black-box testing alone.

Add-on Services

There are several optional services that can be added to the scope of your infrastructure assessment including:

DevSecOps Maturity Assessment – When evolving your Web Applications, there's a risk of vulnerabilities emerging over time. Our solution involves integrating security into the development process, by implementing a practice known as "shifting left" (or DevSecOps), we implement security testing earlier in the applications development. A maturity audit from our security engineers thoroughly reviews the development lifecycle and offers actionable insights to improve your processes or introduce tooling.

Developer Security Training – Security training helps you developers identify and prevent coding vulnerabilities using real-world scenarios in a dedicated lab environment, reducing the risk of application security breaches.

Microsoft 365 Audit

The following table outlines expected service components of your M365 security audit:

Service Component	Description
M365 Security Audit Overview	We will review your M365 environment to validate your security posture of Entra, measuring against industry best practices and CIS benchmarks. This ensures your configurations align with recognised standards for securing users, data, and services.
Identity and Access Management	We will assess your Entra ID setup, including MFA enforcement, conditional access policies, and administrative privilege assignments to reduce identity-based risk and strengthen access control.
Email Security in Exchange Online	We will review your email security posture, including spam filtering, phishing protection (SPF, DKIM, DMARC), and mail flow rules to ensure your users are protected from common email-based threats.
SharePoint and OneDrive Security	We will assess your Microsoft Teams configuration including guest access, external sharing, and compliance settings, to ensure secure and controlled collaboration.
Team Security & Compliance	We will assess you Microsoft Teams configuration, including guest access, external sharing, and compliance settings, to ensure secure and controlled collaboration.
Device Management with Intune	We will review your Intune configuration to ensure policies are in place for device compliance, encryption, application control, and endpoint protection across corporate and personal devices.
Security and Compliance Centre Configuration	We will audit the Microsoft 365 Security & Compliance Center, verifying alert policies, audit logs, role-based access controls, and data loss prevention (DLP) settings to strengthen your governance framework.
Data Governance and Retention Policies	We will review your retention labels and data lifecycle policies to help you manage data securely and ensure compliance with internal policies and external regulations.
Advanced Threat Protection (ATP)	We will evaluate your ATP settings, including Safe Links, Safe Attachments, and treat intelligence features, to enhance detection and prevention of advanced threats across your Microsoft 365 environment.
Audit Purpose and Outcome	We provide a clear summary of misconfiguration that may increase the risk of phishing or data breaches, such as weak SharePoint permissions or Teams/Email gaps, and offer practical remediation steps for rapid improvement.

Cloud Assessment

The following table outlines expected service components of your Cloud Assessment:

Service Component	Description
Security Assessment	We will examine your cloud security controls, configuration, and policies to identify vulnerabilities, ensure alignment with industry standards, and recommend enhancements to protect your environment from threat actors.
Cost Optimisation	We will analyse your cloud resource usage and spending to identify redundant, underutilises, or misconfigured services- helping reduce unnecessary costs while maintain performance and scalability.
Cloud-Native Services	We will assess how effectively your environment leverages cloud-native tools and services, and recommend opportunities to enhance efficiency, scalability, and automation within your cloud platform.
Resilience	We will review your cloud infrastructure for redundancy, failover capabilities, and high availability to ensure operational continuity and resilience against outages or disruptions.
Verify Backup Integrity	We will validate the presence and effectiveness of your backup strategies, confirming that critical data can be reliably restored in the event of data loss, corruption, or system failure.
IAM (Identity & Access Management)	We will audit identity and access policies to ensure least-privilege access, proper role segmentation, and secure authentication practices – reducing the risk of privilege escalation or unauthorised access.
Cloud Segmentation Practices Review	We will evaluate your cloud network segmentation and isolation practices to prevent lateral movement within the environment and enforce secure communication between workloads and services.
Cloud Architecture Design Review	We will analyse your cloud architecture design to ensure it follows secure, scalable, and efficient patterns – highlighting any design flaws or architectural weaknesses.
Infrastructure as Code (IaC) Review	We will review your Infrastructure as Code (IaC) for security, compliance, and operational integrity – ensuring version control, change management, and auditability are properly implemented.

Responsibility Matrix

The following table outlines, at a high-level, the service responsibilities of the client and Aspire.

Service Task	Aspire	Client
Define scope of assessment.	✓	✓
Coordinate assessment delivery.	✓	
Perform penetration testing.	✓	
Provide test schedule and timeline.	✓	*supporting*
Provide access, credentials, and target information.		✓
Approve out-of-scope and restricted areas.		✓
Notify internal teams of testing activity.		✓
Maintain communication during testing.	✓	✓
Document findings and provide final report.	✓	
Clarify technical details from findings.	✓	
Review remediation recommendations.	*supporting*	✓
Implement remediation recommendations.		✓
Retest vulnerabilities (if included in scope).	✓	

Our Experience

Our Customers

Over 2,000 public and private sector customers are delivering citizen services and growing their organisations with us.

Contact Details

At Aspire, our mission is to deliver technology like no other. We have been helping customers to innovate, become more efficient and grow quicker through technology since 2006. Let us help you, too.

Talk to Sales
Interested in our products and solutions but not yet a customer? We'd love to hear from you. Here's how you can reach us.

- Email our Sales Team: hello@aspirets.com
- Call Us: 0330 124 2700
- Visit our website: www.aspirets.com