AIT
partnership group ltd

Protect your organisation

and the people who use your network

Cyber Security Services

At AIT we provide hardware, software and services to protect your organisation and the people who use your network.

When it is unclear where the greatest risk lies our services can identify where you should focus your resources. We help you reduce risk and achieve compliance with regulations and best practice. Our Cyber Security services include the following options:

Cyber Security audit

AIT provides an independent verification of the security of some or all of your systems depending on your needs. The key deliverable is a report highlighting your risks; grading their importance and recommending mitigations.

The Audit is tailored to meet your specific needs. We agree a scope with you during the engagement process and then work with you through 5 stages of the Audit process:

1. Define scope and agree the rules of the engagement, define the success criteria, agree the methodology
2. Design the Audit and select the combination of automated tools, social engineering and manual testing simulating an attacker that will be used
3. Identify targets and landscape that require testing
4. Produce a detailed report of how and why systems were defeated in the test
5. Report includes detailed list of vulnerabilities with recommendations to mitigate them

The Cyber Security Audit may include all or some of the following elements:

Vulnerability scan

A vulnerability scan tests for any weaknesses within your operating systems, applications or critical devices. This includes firewalls and switches which could be exploited by hackers. The vulnerability scan will be carried out on site by our security consultants using internal and external and credentialed and non-credentialed devices.
It will address all areas of the network including:

- Software - scan for weaknesses and unpatched software updates
- Hardware - scan for weaknesses in firewalls and perimeters
- Servers - scan for required updates and cross site scripting
- Website - scan for external and internal hosting vulnerabilities

Penetration testing

A Pentest is an authorised simulated attack on your network to identify weaknesses in your security that could be exploited by a hacker. AIT uses experienced certified ethical hackers (CEH) to undertake the Pentest either onsite, offsite or a combination of both, depending on the scope of engagement. The AIT Pentest will:

- Demonstrate weaknesses in your network and find any gaps in your perimeter
- Provide evidence of best practice approach
- Confirm security features of system components to improve purchasing strategy
- Test web applications and web-based systems

Compliance testing, certification and consultancy

AIT works directly with independent Security Audit and Assessment companies with the following accreditations:

- Payment Card Industry (PCI) Qualified Security Assessor (QSA)
- Cyber Essentials/ Cyber Essentials Plus certification body
- ISO27001:2013 Lead Auditor, Lead implementer
- ISO27005 risk management

This means we provide you with the end-to-end consultancy you need to make gaining key accreditations in GDPR, PCI DSS, Cyber Essentials and ISO27001 simple and painless.

GDPR

The EU General Data Protection Regulation 2018 means that fines of up to £500,000 can be levied by the UK Information Commissioners Office (ICO) if a data subject's rights are breached. Like most EU law it is open to interpretation but it does present a significant compliance risk to organisations holding personal data.

Importantly organisations must be able to demonstrate continuous compliance with GDPR as there is no compliance accreditation or certificate.

The AIT Cyber Security Service offering provides ongoing support to ensure continuous compliance with GDPR. This is achieved through a number of services including;

- ISO27001:2013 accreditation
- Cyber Essentials and Cyber Essentials Plus
- Penetration Testing and Vulnerability Scans
- Security Operations Centre (SOC)
  a managed service offering, using the latest software tools to monitor , detect and respond to threats and identify negligent or criminal behaviours and report on potential data breaches within the 72 hour target specified by GDPR
- GDPR Essentials Scheme
  Topics covered include;
  Data Protection objectives, consent, collection, processing, and safeguarding of personal data, subject requests for access, data portability, data processing, data erasure and use of profiling, training and awareness, complaints and management, review and audits

Payment Card Industry Date Security Standard (PCI DSS)

PCI DSS sets out clear mandatory technical and operational security requirements for organisations accepting or processing or storing cardholder data.

- Scope: we define the cardholder environment and determine the scope for PCI DSS compliance
- Gap analysis: a detailed onsite inspection of your existing cardholder data environment
- Report: detailing all areas of non-compliance
- Remediation: our consultant assists you to address areas of non-compliance
- PCI DSS assessment of the environment
- PCI QSA completion of assessment and compliance documentation
- PCI QSA submission of assessment and compliance documentation along with other requested reports such as vulnerability scans results

Cyber Essentials and Cyber Essentials Plus

Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats. It is required by any supplier to Ministry of Defence and increasingly by those undertaking work for government departments, local authorities and large companies and organisations. It may also reduce your insurance premiums.

The compliance process includes:

- Questionnaire completion and scoping exercise with our consultants
- Gap analysis: identifies where your current systems deviate from the standard with advice on how to close these gaps
- On-site technical verification and internal and external vulnerability scans
- Report of findings for the accreditation body
- Arrangement for the Cyber Essentials or CE Plus certificate to be issued

ISO27001

ISO27001:2013 is the international standard for Information Security and involves implementing and maintaining an Information Security Management System (ISMS). It provides evidence of best practice and is often a requirement in tenders and supplier agreements and helps organisations meet their General Data Protection Regulation requirements (GDPR).

The compliance process includes:

- Analysis and scope of what is required to implement and maintain the standard
- Identification of key risks around them
- Development of processes and controls to mitigate risk and protect assets
- Maintain the cycle of PLAN, DO, CHECK, ACT to ensure you are continually optimising your ISMS

Why use AIT Cyber Security Services

- Trusted advisors to Public Sector and Blue Chip clients since 2002
- Our team of network professionals has in depth hands on experience of network security issues in Wi-Fi, IoT and edge and core network infrastructure
- AIT is ISO27001, 9001, 14001, 18001 and Cyber Essentials certified
- AIT only engages with independent, fully qualified cyber security and compliance consultants which means you are assured of the highest quality advice, feedback and certification
- AIT uses certified ethical hackers (CEH) with experience of how to interpret the results and identify how you could mitigate your risks against exploits
- AIT provides direct access to leading Cyber Security Consultants so you can tap into their knowledge to gain additional insights into how you can improve your cyber security practices