YOUR CYBER THREAT. **MITIGATED.**

ARISTI
G-CLOUD 14 SERVICES DEFINITION

15 APRIL 2024

Aristi Limited, Innovation Centre, 1 Devon Way, Longbridge Technology Park, Birmingham B31 2TS
Web: www.aristi.co.uk Email: info@aristi.co.uk Tel: 0121 222 5630

1 CONTENTS.

1 Contents. 1
2 Introduction 2
2.1 Overview 2
2.2 Contact Details 2
3 Services Definition 3
3.1 PSN services 3
3.1.1 PSN Support Services 3
3.1.2 PSN IT Health Check 4
3.2 Penetration Testing (non-CHECK service) 4
3.3 Cyber Essentials 5
3.4 Cloud Security Assessments 5
3.5 Red Team Assessments 5
3.6 Physical Security Assessments 6
3.7 Information Assurance 6
3.8 Data Protection 6
3.9 ISO/IEC 27001 Compliance 7
3.10 Security Awareness Training 8
3.11 Cyber Security as a Service 9

2 INTRODUCTION

2.1 Overview

Aristi Limited (Aristi) delivers various Specialist Cloud Services to support clients in the public, private and third sectors to implement robust and sustainable Information Assurance (IA) initiatives.

Our consultants are security cleared to SC and NPPV and hold a range of qualifications including CHECK Team Leader, CHECK Team Member and ISO 27001 Lead Auditor. They have extensive experience of delivering successful IA projects and embedding good security practices within organisations that add real value rather than 'tick box' compliance.

Our approach is based on collaboration and knowledge sharing with our clients such that we became trusted security partners. As an SME, we are able to offer bespoke services and quickly adapt to changing client requirements.

Our services are based on real world experience of supporting our clients to improve security postures and comply with national Codes of Connection for PSN, PSNP and Airwave. We provide bespoke services for supporting organisations to transition to cloud services as well as managed services to help keep cloud services secure.

2.2 Contact Details

We would be happy to help with any enquires or requirements you may have. Our contact details are provided below.

Email: info@aristi.co.uk

Tel: 0121 222 5630

Address: Aristi Limited
Innovation Centre
1 Devon Way
Longbridge Technology Park
Birmingham
B31 2TS

Web: www.aristi.co.uk

3 SERVICES DEFINITION

3.1 PSN services

Our PSN services will help you achieve and maintain your connection to PSN compliant cloud services.

3.1.1 PSN Support Services

The PSN is a single network, based on industry standards. It provides a foundation for government ICT and is implemented across the UK public sector. The network allows government departments and other public sector organisations to share services safely and work together more efficiently.

The PSN for Policing (PSNP) is the replacement for the Police National Network (PNN3) family of networks (CJX, xCJX and SCN) and associated services, which enable most operational policing activities.

Aristi has been working with public sector (including emergency services) clients for over 15 years providing support for compliance with national standards and Codes of Connection.

Our consultants have extensive experience of PSN requirements as well as compliance with the Cabinet Office Security Policy Framework (SPF). We have developed a number of services to help public sector clients procure new PSN connectivity or to maintain compliance with PSN security requirements.

We can also support network service providers within the PSN Inter-Provider Encryption Domain (IPED) to meet the IPED obligations to keep networks secure. This includes helping providers to meet the requirements of the NCSC guidance on using IPSec to protect data.

Our services include:

- PSN Readiness Gap Analysis

  The PSN Readiness Gap Analysis is designed to quickly establish the current security posture of the organisation and determine what is required to comply with the PSN/PSNP CoCo. The output is a detailed report together with recommendations and a suggested development plan for achieving compliance.

  The analysis covers physical, technical and procedural controls as well as a review of existing security policy documentation.

- PSN Compliance Support

  Support can be provided for:

  - Information Assurance strategy development to support PSN and help realise the benefits of PSN;
  - PSN Business Case Development;
  - PSN Procurement support including establishment of PSN requirements and evaluation of suppliers;
  - Technical architecture review and design to meet NCSC secure design principles and PSN CoCo requirements;

- Development of security policies and procedures;
- Completion of the PSN CoCo;
- Business Impact Assessments;
- Technical Risk Assessments;
- Development of Risk Management documentation and Remediation Action Plans.

3.1.2 PSN IT Health Check

The PSN CoCo requires organisations to implement an annual programme of IT Health Checks to validate equipment not provided as part of a PSN service that interacts with PSN services. This involves a vulnerability analysis of the IT infrastructure that is established as in scope for PSN connectivity.

Aristi consultants are certified under the Cyber Scheme to provide PSN compliant IT Health Check services. These services are designed to identity technical vulnerabilities in IT systems which may result in compromise of the information held on the systems. The tests include applications, servers, firewalls and network equipment such as routers and switches. Tests can be conducted internally on local area networks and externally from the Internet.

The results of the tests are documented in a detailed report together with recommendations for mitigating the risks identified.

3.2 Penetration Testing (non-CHECK service)

Aristi Cyber Scheme certified experts will study your network and applications and search for vulnerabilities. This is achieved through the use of semi- automated tools, script execution and is heavily dependent on manual testing and verification techniques. By analysing the results, our consultants will expose potential vulnerabilities and customise subsequent tests, based on the initial findings.

The penetration test can include the further exploitation of vulnerabilities that are discovered (chained exploits), if explicitly requested by the client.

Options for network penetration tests include:

- **External Penetration Test** – Conducted remotely on external or public facing networks or applications (using OWASP methodology) to identify vulnerabilities that are visible to attackers over the Internet;
- **Internal Penetration Test** – Conducted on the internal network to identify vulnerabilities that are visible to insiders, contractors and partners with potential malicious intent.

Penetration Testing of cloud hosted services is very important. Whether your utilising PaaS, IaaS or SaaS, all have security implications for your network or data. Aristi's cloud ready penetration testing methodology focuses on identifying the services you are using and their relationship with your organisation. It evaluates the technical relationship between your environment and cloud services allowing more assurance to be obtained about the severity posture and potential risk from both the internet and the connected cloud infrastructure.

Any vulnerability discovered will be analysed and categorised alongside a detailed recommendation that will enable the client to take remedial action and mitigate the issue. Upon completion of a penetration test, the client is provided with a test report which summarises the identified vulnerabilities and advises on solutions that will improve security.

3.3 Cyber Essentials

The Cyber Essentials scheme provides businesses with clarity on good basic cyber security practice. It enables your company to be better protected from the most common cyber threats. Cyber Essentials is not limited to companies in the private sector but is also applicable to public sector organisations of all sizes.

Aristi is a Cyber Essentials Certification Body and can provide support for both Cyber Essentials and Cyber Essentials Plus compliance. Our consultants are qualified Cyber Essentials assessors who specialise in Cyber Security. We can help your organisation to comply with the requirements of Cyber Essentials and achieve formal certification against the standard.

3.4 Cloud Security Assessments

Our Cloud Security Assessment is designed to assess your cloud hosted services for security weakness including misconfigurations, that can be exploited by an attacker to gain access to your service. We can assess the configuration of your Microsoft 365, Azure or AWS cloud environments and provide recommendations to help reduce your cyber risks.

3.5 Red Team Assessments

Our Red Team assessments are goal-based, where we attack just like a real-world adversary using real world techniques to gain access to an agreed target within your cloud environment.

The benefit of conducting such an assessment is that it tests your defenders (people) as well as your defences (technology). It also tests your ability to detect and defend against a realistic and relevant attack as we take into account your risk environment and build attack scenarios that are most likely to occur in your business sector.

Many organisations rely on traditional penetration testing to protect services. Although penetration testing is a key component of a cyber security strategy, it assumes that the attacker has access to your IT environment, has credentials and can run scanning tools undetected. Real world attacks do not occur in this manner so a Red Team assessment can add value to your penetration testing regime.

Our Red Team assessment can also test the effectiveness of your alerting, logging, and monitoring systems, whether they are in-house or outsourced to a Managed Security Service Provider (MSSP).

Our dedicated Red Team, have a vast and wide-reaching level of expertise in the cyber security industry. We align our Red Team operations to not only industry standards such as MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) and NIST Cybersecurity framework but also to the cutting edge real world tactics used by our adversaries. This ensures you get a professional consistent service which is as close to a real-world attack as possible using all the latest tactics, techniques and procedures and threat emulation.

3.6 Physical Security Assessments

Our Physical Security Assessments help organisations to understand, document and manage access to networks and information systems that support the operation of essential functions including cloud hosted environments.

Physical security assessments provide confidence that the physical security measures employed by your organisation or your provider are sufficient to protect against unauthorised access, tampering, theft or reconfiguration of systems.

Our assessments are tailored to your risk environment and utilise the same tactics, techniques and procedures that an attacker would use.

3.7 Information Assurance

We offer a range of cyber security consultancy services to support IT transformation projects, security improvement initiatives and standards compliance.

We have acted as independent assurers on national programmes providing risk assessments, specialist security advice and guidance to technical design teams and business stakeholders. We also act as trusted security advisors to organisations, sitting on Security Boards and Security Forums/Working Groups.

Our consultants have many years of experience working with some of the most sensitive data and systems in the UK. Each engagement is tailored to the specific needs of our client to ensure we add real value.

Having a good security culture embedded within a business is a key part of any organisation's cloud strategy. We utilise a number of frameworks to support the development of good security governance within your organisation including ISO 27001, NIST, and the NCSC Cyber Assurance Framework (CAF).

In addition to the above, we also provide specialist services such as:

- Cyber Resilience exercises to assess your ability to respond to a cyber-attack.
- Business Continuity Exercises to assess your ability to respond to an event that disrupts normal business activities.
- Cyber Incident Response to provide post incident guidance.

3.8 Data Protection

Our Data Protection services are designed to support organisations to meet the requirements of GDPR and the UK Data Protection Act. We can provide assessments to identify gaps, Provide support to develop procedures and policies to meet GDPR requirements, provide user awareness training and conduct audits to help maintain compliance.

Our Data Protection as a Service provides a 'critical friend' to you to call when you require support for data management or if you have a data breach. We can act as your Data Protection Officer and provide independent verification of your compliance against GDPR.

3.9 ISO/IEC 27001 Compliance

ISO/IEC 27001 is the only auditable standard that provides a framework for establishing an Information Security Management System (ISMS). Certifying your ISMS against ISO 27001 can bring the following benefits to your organisation:

- Demonstrates the independent assurance of your internal controls and meets corporate governance and business continuity requirements;
- Independently demonstrates that applicable laws and regulations are observed;
- Provides a competitive edge by meeting contractual requirements and demonstrating to your customers that the security of their information is paramount;
- Independently verifies that your organisational risks are properly identified, assessed and managed, while formalizing information security processes, procedures and documentation;
- Proves your senior management's commitment to the security of information held by the organisation;
- The regular assessment process helps you to continually monitor your performance and improve.

Our objective is to reuse as much of your existing investment in security policies and procedures as possible. In order to achieve this, our approach is based on working with you to understand what has been achieved to date, update and implement policies and procedures as required to meet the standard, develop an Information Security Management System (ISMS) and implement a security awareness program to enforce compliance.

Our approach is based on the following activity:

- Understand your business, processes and procedures;
- Work with you to define a scope for the ISMS in relation to key assets and business processes. This will form the basis for the subsequent compliance implementation activities;
- Review the existing asset list and risk assessment methodology and use this or suggest an alternative as required to conduct a risk assessment against the ISMS scope. Determine appropriate management action and priorities for managing information security risks;
- Review the existing security policy documents, update them as required to meet ISO/IEC 27001 requirements and work with you to implement the policies;
- Develop a Statement of Applicability and provide advice and guidance on the selection and implementation of adequate and proportionate security controls such as policies, procedures and technical functions;
- Develop and deliver a security awareness program to your staff;
- Provide advice and guidance on the creation of a 'security culture' within your business;

- Once all the requirements of ISO/IEC 27001 have been met, conduct an independent audit against the standard and document the findings in a formal report. Provide a certificate of compliance.

ISO27001 consultancy services include:

- Gap Analysis
- Risk Assessment
- Risk Remediation/Treatment Plans
- Development of Statement of Applicability (SOA)
- Development of security policies and procedures
- Awareness Training
- Management Presentations
- Pre-certification Audits to ISO/IEC 27001

Our consultants are qualified ISO/IEC 27001 Lead Auditors with many years' experience of delivering information security services. We can help your organisation to comply with the requirements of ISO/IEC 27001 or achieve formal certification against the standard.

3.10 Security Awareness Training

In order for organisations to implement effective IA, a governance structure must be developed and embedded within the business. This requires senior management support to change the culture of the organisation so that good security becomes the norm. Key to this is the identification and training of specific roles such as:

- Senior Information Risk Owner (SIRO)
- IT Security Officer (ITSO)
- Information Asset Owners (IAO)

Aristi can provide training for these key roles as well as general security awareness training for staff. Training can be provided on site, remotely over MS Teams or at our training facilities in Birmingham. All training courses can be tailored to reflect specific requirements and can be based on your organisation rather than generic theory.

3.11 Cyber Security as a Service

Our Cyber Security as a Service (CSaaS) goes beyond a business relationship, providing a true partnership with your organisation. It delivers a managed cyber security service that is tailored to your business needs, your exposure to cyber risk and your technical environment. Outsourcing your cyber security to our experts allows you to focus on your core activities.

Key benefits include:

- Access to Cyber expertise
- Cheaper than building an inhouse team
- Fixed monthly costs helps with budgeting
- Improves cyber maturity and reduces your exposure to cyber risk
- Scalable – you can add more services as required, or remove services that are no longer needed

CSaaS includes a range of cyber services tailored to your specific needs including:

- Continuous testing to identify security weaknesses in your cloud hosted systems
- Security Maturity Assessments based on NIST, ISO 27001 and GDPR to assess your security posture and build security improvement plans
- Cyber Resilience exercises to assess and help improve your ability to respond to security and business continuity incidents
- Phishing assessments
- Subject matter expertise at your security board or security forum meetings
- Managed security incident detection and response services

-- End of Document --