



# Cyber Security Consultancy

## G-Cloud 14 Service Description

Arculus Ltd: Company Registration Number:13158390

Registered Address: The Old Casino, 28 Fourth Avenue, Hove, East  
Sussex, BN3 2PJ, United Kingdom

# 1. Overview

Arculus provides high quality cyber security consultancy services. Our team has worked with organisations to achieve cyber security outcomes in a wide variety of complex and diverse environments. We are an NCSC Assured Cyber Security Consultancy (ACSC) provider for all services: Security Architecture, Risk Management, and Audit and Review. Outcomes include achieving certification to a chosen standard including ISO/IEC27001, Cyber Essentials and Cyber Essentials Plus. We have developed and implemented information risk management processes which support the clients' governance model as well as the implementation of controls which are targeted to treat specific defined and quantified risks. This approach ensures that the level of security controls is in line with the context of the organisation, the risk appetite of the organisation and the level of cyber threat faced by that organisation.

Our consultants are experienced and qualified. Many of our team are former CLAS consultants with an up-to-date approach to effective and proportionate risk management. Our team is qualified under the NCSC Certified Cyber Professional Scheme and hold qualifications including CISSP, CISM and ISO/IEC 27001 Lead Auditor and Lead Implementer.

Our cyber security consultancy engagement process is aligned to the NCSC Certified Cyber Security Consultancy Standard, ensuring a high-quality client journey including agreed deliverables, clear and regular reporting, defined escalation paths, suitably skilled and qualified resources and focused delivery.

## 2. Services

### 2.1 Security Architecture Consultancy Services

Security architecture and risk assessment are tools used to understand the risks to the organisation or a particular project. Arculus can provide support and guidance including managed security services. Arculus have consultants available with CCP Lead and Senior SIRA, Senior Architect, SABSA / TOGAF, ISO27001 certified.

Our consultants are proficient in many risk methodologies, including ISO27005, IS1&2, IRAM. Experts in NCSC Cloud Security Principles, supplier assurance and NCSC CAF plus CNI requirements.

The common output, a prioritised list of risks, can be used to drive decisions on how the organisation or project should progress, which is then used as an input into the risk management process. If all of the risks above the organisational or project's risk management tolerance are then properly managed, there is an increased likelihood of success moving forward.

Arculus's experienced Security and Information Risk Advisors can deliver quantitative or qualitative risks assessments using a variety of methodologies and frameworks to fit your requirements, including the use of:

- NIST SP 800-30
- CRAMM / CRAMM Express
- Risk IT / COBIT
- IRAM
- ISO 27000 series guidance on risk and management

## 2.2 Managed Security Service - Risk Assessment & Architecture

Arculus can offer active, on-going management of information security to ensure information assets are appropriately protected and that legal and regulatory compliance requirements are met. This includes:

- Risk assessments, to identify risks faced by each organisation
- Consultancy on securing systems and services
- Gap analysis and audit of compliance with recognised security standards such as ISO27001
- Advise on or producing a business case for introducing security controls
- Security incident prevention and management

Service benefits include:

- Highly experienced UK-based consultants
- Experienced security testing and assurance teams with wide, varied experience
- As independent information security specialists, we provide unbiased services
- Advice and recommendations given with a truly holistic security view
- ISO27001 and ISO9001 certified
- All deliverables independently quality assured reviewed
- Increased compliance, whilst reducing risks to reputation damage

The Arculus Managed Security Service provides the full range of skills required to assure and manage security across your organisation on an on-going basis.

## 2.3 Cloud Supplier and Consumer ISO27001 Support Including ISMS creation and Internal Auditing

Arculus has the skills and experience to assist in the implementation and ongoing management of your ISO27001, we have successfully implemented and managed numerous ISO27001 ISMS's for small businesses and larger organisations alike.

Arculus can provide support for organisations who are looking to implement an ISO27001 ISMS, gain ISO270001 certification or who already have an ISO27001 ISMS within the organisation.

## 2.4 Consultancy Services:

Full ISO27001 Certification Support, advice, guidance and consultancy support covering all of the requirements from scoping through to certification for businesses of all types, sectors and sizes.

- Scoping, planning and budgeting
- Securing senior management and board commitment
- Identifying interested parties, legal, regulatory and contractual requirements
- Performing risk assessments
- Providing advice on control implementation
- Developing internal competence and assigning responsibilities
- Reviewing management system documentation, policies and procedures
- Conducting staff awareness training
- Auditing, monitoring and reviewing the current ISMS
- Certification audit support
- Specific ISO27001 Milestone Consultancy Support
- ISO27001 Gap Analysis
- ISO27001 Internal Audit

## 2.5 Payment Card Industry Data Security Standard (PCI-DSS) Consultancy

The Arculus service portfolio provides ongoing PCI DSS compliance and maintenance as part of an organisation's overall business-as-usual (BAU) security strategy.

Our trusted methodology is defined by the following six key phases:

- Define and validate the scope of any assessment.
- Determine the level of compliance against the PCI standard and carry out a risk assessment for the cardholder data environment.

- Remediation action planning
- Apply remediation skills and experience for implementation of security policies, development of processes and procedures and designing technical infrastructures to secure the data environment.
- Conduct an independent audit or support of self-assessment questionnaires (SAQ).
- Penetration Testing & Quarterly Vulnerability Scanning for compliance management

## 2.6 Technical Architecture Services Cloud Specialists

Arculus will provide analysis of your technical landscape and company strategy to recommend the best way of moving operations and applications into a Cloud-based infrastructure and benefit from operational improvements and cost savings.

We can guide your organisation to produce a Cloud-based architecture strategy and supporting artefacts for the current and future state.

Features:

- Architectural Review
- Technical Debt Review
- High level cloud strategy
- Cloud architecture design
- Cost models
- Roadmap to the Cloud
- Consultancy services to support Microsoft cloud/Azure selection/implementation
- Make appropriate cloud-architecture decisions for your needs
- Maximise benefits from cloud-hosting

## 2.7 Data Privacy and Virtual Data Protection Officer (DPO) Services

The Virtual Data protection officer (vDPO) service is typically adopted by organisations who do not have a specialist resource internally, where a full-time role is not a viable cost option.

The provision of this service can commence once Arculus has completed an initial assessment or understands your organisations data protection readiness.

The GDPR requires organisations to have a DPO if they meet certain criteria. Arculus vDPO service is designed to provide organisations with skilled and qualified consultants to meet the requirements of the DPA/GDPR, as well as deal with Subject access rights requests and help in ensuring that internal artefacts are in place and kept up to date with changing legislation.

Outsourcing the requirement for certified GDPR/DPA resource allows businesses to focus on internal objectives while remaining compliant.

The Arculus vDPO service can provide:

- Assistance in meeting the compliance requirements of the DPA/GDPR
- Relieve the burden on internal resource currently used to meet compliance requirements and deal with Subject rights requests
- Stay abreast of developments with data protection legislation changes
- Meet the requirement to have a qualified resource to deal with DPA/GDPR related tasks for the business
- Assist in keeping required internal documentation reviewed and up to date

## 2.8 Business Continuity Management & Disaster Recovery Services

Arculus can support your organisation to assess the business impacts and risks of a disruption. We can advise on leadership and governance, assess impacts and risks, aid in the development of plans and solutions, training of your employees and testing of plans and solutions to give your organisation and its customers the assurance it needs.

The range of services we can offer includes:

- Carry out analysis of the current state of business continuity management within your organisation to show where the gaps are and where improvements can be made
- Support implementation of frameworks, policy, objectives, solutions and plans to improve the maturity of your business continuity management
- Implementing of internationally recognised standards for business continuity management such as ISO 22301 and Business Continuity Institutes Good Practice Guide
- Host workshops for business impact analysis and risk assessment, ensuring you identify your critical business services and what downtime could be tolerated
- Provide advice for solutions and support the production of plans to mitigate risks
- Develop testing and exercise strategies and schedules as well as supporting the production of testing and exercise results
- Provide training and support for all employees to ensure they know what they have to do during a disruption
- Provide training and workshop initiatives to build your in-house capacity and capability to support your ongoing business continuity management initiative
- Support ongoing review of your business continuity management by carrying out internal reviews, establishing measurement monitoring activities aligned to strategic objectives, and facilitating continual improvement

- Provide advice on applicable frameworks to support your organisation to effectively manage and govern business continuity management
- Support the identification of relevant legislation, regulations, standards and best practice applicable to your organisation
- Undertake reviews and reporting of business continuity management ensuring that risks have been identified, and that plans to mitigate are progressed and effective

## 2.9 Third Party Assurance Services

Arculus can support organisations in assessing the risks associate with the third-party processing of their data. Arculus can advise on governance, technical and organisational controls, and offer remediation guidance for compliance, as well as providing support for existing third-party arrangements and future procurement activity.

The range of services we can offer includes:

- Support compliance with applicable standards and legislation such as UK Government Supplier Assurance Framework, Data Protection Act 2018, General Data Protection Regulation, ISO/IEC 27001 etc.
- Support for existing outsourced services in the identification of all third-party arrangements including those third parties that sub-contract services
- Provide advice on applicable frameworks to support your organisation to manage and govern existing and new third-party contracts
- Provide support when implementing frameworks, policies and processes to improve the maturity of supplier assurance management
- Support legislation, standards and best practices applicable to each outsourced service type
- Perform a review of compliance against relevant legislation, standards and best practice
- Identify a suitable audit approach such as independent third-party audit
- Perform necessary risk assessments, so that your organisation understands the residual risks relating to each outsourced arrangement
- Identify appropriate and proportionate remediation activities to improve security maturity
- Support development or improvement of non-functional requirements, security policies, contract clauses, service provision model and remote access approach
- Review of business-as-usual services provided by third parties such as vulnerability management, lifecycle management, risk remediation and protective monitoring.
- Provide training and workshop initiatives to build your in-house capacity to manage supplier assurance
- Experienced and qualified UK-based consultants, including NCSC Certified Cyber Professionals, with government, public sector and wider industry experience, providing trusted advice.

## 2.10 Virtual CISO vCISO

Informed and experienced cyber security leadership is critical to organisations as they address cyber security challenges. The right leadership will communicate with top management as well as in house resources and external partners ensuring clarity of purpose and a proportionate response. This leadership can mean the difference between the success and failure of an organisation.

Not every organisation needs a full time Experienced Chief Information Security Officer to succeed. In many cases reliance on an external trusted expert is a better solution.

Arculus virtual Chief Information Security Officer (vCISO) resources have a wealth of experience in providing leadership and expertise to organisations across public and private sectors. We have excellent understanding of technical aspects of cyber security and the ability to communicate effectively to board level. We can help organisations to address the cyber security agenda effectively from the board to the end user.

Our vCISO resources are offered on a flexible basis for maximum efficiency. We nominate a regular resource to build relationships with stakeholders and provide clear and concise advice and guidance at strategic and tactical levels.

## 2.11 SOC2 Audit Consultancy and Certification Services

The System and Organisation Control (SOC) 2 compliance focuses on one or any combination of the AICPA's Trust Services Criteria including Security, Availability, Processing Integrity, Confidentiality, and Privacy, depending on the context of the organisation in scope. Achieving SOC 2 compliance demonstrates the organisation's commitment to cybersecurity best practices. This provides customers and stakeholders assurance in the service or organisation.

SOC 2 reports are unique to each organisation. In line with specific business practices, each designs its own controls to comply with the standard. There are two types of SOC reports:

- Type I (often referred to as a point-in-time report) describes a vendor's current systems and whether their design is suitable to meet relevant trust principles. Subsequent type 2 reviews often use the initial Type I report as a starting point.
- Type II (often referred to as a period-of-time report) details the operational effectiveness of those systems and assesses how they are implanted on an ongoing basis.
- These internal reports provide you (along with regulators, business partners, suppliers, etc.) with important information about how your service provider manages data.

Arculus can support your organization through the full journey to achieve SOC 2 compliance and certification by guiding you through the entire audit process and providing the full certification service through our AICPA partnerships.



## 2.12 Security Awareness Training

Security awareness is critical to an effective cyber security control set. People are widely targeted by attackers either at random or specifically. Attackers seek to exploit weakness in peoples understanding of how they work. By giving people the information, insight and awareness to identify potential pitfalls such as phishing emails, scam web sites or the tactics and techniques and procedures used by attackers they are empowered. Successful security awareness training is the difference between users being a weakness to users being the first line of defence against cyber security attacks.

Arculus is experienced in providing security awareness training to the general user community, specific user groups such as developers and to senior leadership. Training is targeted to ensure that it is relevant and accessible. We provide background information on the types of attack, why attackers act as they do and how to spot the give-away signs that betray an attempted attack.

We are able to combine awareness training with other services such as red teaming, where social engineering and open-source intelligence are used to target users, and simulated phishing attacks, bringing the messages to life for users at all levels. Our reports on awareness training and attainment by the users are used as evidence to support ISO/IEC27001 compliance or fulfilling legal and contractual requirements.

## 3. About Arculus

Founded in 2021 by 3 highly experienced consultants, Arculus is a specialist, independent Cyber Security consultancy. We provide Cyber Security advisory services including conducting Cyber Assessments, Information Risk Management and Assurance, SOC2 consulting and certification, ISO/IEC27001 services, and Data Privacy consultancy.

Our consultants hold industry leading qualifications including NCSC Certified Cyber Professional Scheme (CCP), CISSP, CISM and ISO/IEC27001 Lead Auditor.

Our Penetration Testing and Vulnerability Assessment services are accredited by CREST, a global body ensuring the highest standards of testing and qualifications.

We are NCSC CHECK and CREST-accredited for penetration testing and vulnerability scanning and are specialists in Red Teaming and device-testing and are a Cyber Essentials/Plus Certifying Body. We are able to carry out all types of penetration testing including Web Application, Infrastructure, Cloud based services, Red Teaming and Device Testing.

We can help you secure your digital transformation through our pragmatic solutions, guidance and services. We have a proven track record of successful security outcomes in complex and challenging environments.



## 4. Contact

**Tel:** +44(0)845 299 3009  
**Email:** [info@arculus-cyber.co.uk](mailto:info@arculus-cyber.co.uk)  
**Web:** <https://arculus-cyber.co.uk/>  
**Post:** Arculus Limited  
The Old Casino  
28 Fourth Avenue  
Hove  
East Sussex  
BN3 2PJ  
United Kingdom

Arculus Ltd: Company Registration Number:13158390

Registered Address: The Old Casino, 28 Fourth Avenue, Hove, East Sussex, BN3 2PJ, United Kingdom