G-Cloud 15 Lot 3 - Cloud Support
GRC Services Overview

Prism Infosec

Prism Infosec supports organisations globally to prepare for, respond to and manage cyber security threats.

Governance, Risk & Compliance

Confidence built on control

Cyber security is more than a technical challenge, it's a governance, risk and compliance challenge too. Our GRC and security consulting services give you expert-led support to help align your security practices with business objectives to meet regulatory demands and reduce organisational risk with confidence.

We combine strategic insight with practical advice to help you make the right decisions, based on your risk profile and operational realities.

We don't just support with your compliance challenges, we help you to build a security posture that's right for your business and its growth. It's grounded in best-practices and tailored to you. Our approach is personal and built on decades of experience.

Our experienced consultants become an extension of your team, helping you embed effective controls, demonstrate compliance and strengthen resilience - without unnecessary complexity.

Service name	Description
GovAssure	GovAssure is the UK Government's cyber assurance framework for assessing and improving the cyber resilience of public sector organisations. This service provides structured support to help organisations meet GovAssure requirements, demonstrate compliance, and improve their overall security posture in line with government expectations. The service begins with a maturity assessment against GovAssure outcomes, covering governance, risk management, protective security, incident response, and operational resilience. Evidence is gathered through interviews, documentation reviews, and technical validation to establish a clear baseline of current capability. Organisations receive a detailed report highlighting strengths, gaps, and areas of non-compliance, along with a prioritised improvement roadmap. Ongoing support can include remediation planning, policy development, assurance reporting, and preparation for formal assessments. GovAssure services help public sector bodies demonstrate accountability, manage cyber risk effectively, and maintain confidence with central government stakeholders.
ISO27001 Compliance	ISO 27001 Compliance services support organisations in implementing, maintaining, and certifying an Information Security Management System (ISMS) aligned with the ISO/IEC 27001 standard. The service provides a structured, risk-based approach to managing information security across people, processes, and technology. The engagement typically includes gap analysis, risk assessment, control selection, policy development, and implementation support. Organisations are guided through the creation of required documentation, governance structures, and operational procedures to ensure compliance with ISO 27001 clauses and Annex A controls. Additional support includes internal audits, management reviews, and certification readiness assessments. The service helps organisations not only achieve certification but also embed continuous improvement, ensuring that information security remains aligned with business objectives, regulatory obligations, and evolving threat landscapes.
PCI Qualified Security Assessor (QSA) Services	PCI Qualified Security Assessor (QSA) Services provide independent, accredited assessment of compliance with the Payment Card Industry Data Security Standard (PCI DSS). These services are required for many organisations that store, process, or transmit payment card data. A QSA conducts a formal assessment of technical controls, policies, procedures, and security processes across the cardholder data environment. This includes reviewing network security, access controls, encryption, monitoring, vulnerability management, and incident response capabilities. Deliverables include a Report on Compliance (ROC) or Attestation of Compliance (AOC), providing assurance to card schemes, acquirers, and business partners. PCI QSA Services help organisations reduce the risk of card data breaches, avoid financial penalties, and maintain trust with customers and payment providers.
PCI-DSS Compliance Services	PCI-DSS Compliance Services support organisations throughout the entire compliance lifecycle, from initial scoping and gap analysis through to remediation and ongoing compliance management. The service helps define the cardholder data environment, assess current controls against PCI DSS requirements, and identify technical and procedural gaps. Support is provided for remediation planning, control implementation, documentation development, and staff awareness. Ongoing services may include vulnerability scanning, policy reviews, internal audits, and preparation for QSA assessments. These services ensure compliance is sustainable, reducing risk, protecting payment data, and maintaining operational efficiency.

Service name	Description
Policy Review and Development	Policy Review and Development services ensure that organisational policies accurately reflect current risks, regulatory obligations, and best practices. This service supports the creation, review, and enhancement of cyber security, data protection, and governance documentation. Existing policies are assessed for completeness, clarity, alignment with standards (such as ISO 27001, NIST, or NCSC), and real-world applicability. Gaps, inconsistencies, and outdated content are identified and addressed. New policies, procedures, and standards are developed to support secure operations, regulatory compliance, and organisational accountability. This service ensures staff understand their responsibilities, supports audit readiness, and strengthens overall governance and risk management.
Virtual CISO	The Virtual Chief Information Security Officer (vCISO) service provides organisations with access to senior-level cyber security leadership without the cost or commitment of a full-time executive. The service is designed to support organisations that require strategic oversight, governance, and expert guidance to strengthen their security posture and manage cyber risk effectively. The vCISO works closely with executive leadership, IT teams, and key stakeholders to develop and deliver a tailored cyber security strategy aligned with business objectives, regulatory requirements, and risk appetite. This includes defining security roadmaps, establishing governance frameworks, overseeing risk management processes, and ensuring that security initiatives are prioritised appropriately. The service also provides leadership across incident preparedness and response planning, security policy development, supplier risk management, and assurance activities such as audits and compliance programmes. Regular reporting to senior management and boards ensures visibility of cyber risks, performance metrics, and improvement progress. By providing experienced, independent security leadership, the Virtual CISO service helps organisations build resilience, improve decision-making, and demonstrate effective cyber governance to customers, regulators, and stakeholders.
AI Policy Review	The AI Policy Review service helps organisations establish clear, compliant, and effective governance for the use of artificial intelligence technologies. As AI adoption increases across business operations, this service ensures that policies align with legal, ethical, security, and operational requirements while supporting innovation in a controlled and responsible manner. The service begins with a review of existing AI-related policies, procedures, and guidance, including acceptable use, data handling, security controls, and third-party AI usage. Where formal AI policies do not yet exist, the service supports the development of new policy frameworks tailored to the organisation's risk profile, sector obligations, and strategic objectives. The review assesses alignment with relevant regulations, standards, and best practice guidance, such as data protection requirements, intellectual property considerations, transparency expectations, and emerging AI governance frameworks. It also evaluates how AI risks - including bias, data leakage, model misuse, and security vulnerabilities - are addressed within organisational controls. Deliverables include a detailed gap analysis, clear recommendations for improvement, and updated or newly developed AI policies and procedures. The AI Policy Review service helps organisations manage AI-related risks, demonstrate responsible governance, and ensure AI is used securely, ethically, and in line with business and regulatory expectations.

Prepare

Prepare your organisation for cyber security threats.

Prepare your organisation for cyber security threats. Understand your current posture and strengthen your defences. We can help you get ahead of the risks with tailored testing, preparedness services and red teaming.

- Cyber Security Assessments & Penetration Testing
- Cloud Security
- Red Teaming & Simulated Attack
- Regulated Testing Schemes

Respond

Respond effectively to cyber security incidents.

Take control when incidents strike and recover with the confidence to move forward. Specialist support to help you respond to cyber threats and restore operations quickly.

- Remediation Services
- Incident Response
- Digital Forensics

Manage

Manage your ongoing cyber security resilience.

Build long-term resilience with ongoing support and consultancy. From strategic governance to fully managed SOC services and incident response retainers.

- Managed Security Services
- GRC & Security Consulting
- Compliance Services
- vCISO

About Prism Infosec

Prism Infosec is an Information Security company based in Cheltenham and Liverpool and was founded in 2006. The Company has delivered information security consultancy and assessment services to some of the world's largest organisations including private enterpise, public sector, government, defence and healthcare. Uniquely, Prism Infosec's consultants possess both a business and management focus, but also a diverse range of technical skills. Whether delivering advice on cutting edge information security architectural solutions, conducting management controls audits, or in-depth technical penetration testing, our consultants always deliver a quality end-to-end service.

To book an assessment call:
+44 (0) 1242 652100

Send us an enquiry email:
contact@prisminfosec.com