Amethyst

Making Cyber Secure™

UNDERSTANDING OUR SERVICES

ABOUT US

Amethyst Risk Management is a leading cybersecurity company, with a proven 100% customer satisfaction track record.

We have developed a reputation for succeeding where others have failed, delivering on time and to budget, without compromising on quality.

18
YEARS IN BUSINESS

100%
CLIENT SATISFACTION

96%
REPEAT BUSINESS

1
UNITED TEAM

100%
SECURITY CLEARED PERSONNEL

OUR MISSION

Our mission is to provide expert cybersecurity and risk management services that ensure the protection and resilience of our clients' digital infrastructures. By combining industry-leading expertise with an unwavering commitment to excellence, we deliver innovative, tailored solutions that exceed our clients' expectations.

OUR SERVICES

To ensure we provide the most effective and relevant solutions, our services are thoughtfully organised into three distinct categories.

Cybersecurity Certification and Governance, Risk & Compliance (GRC)

Our expert consultants can support your compliance management and assurance for many standards and frameworks.

Cybersecurity for Enterprises, Programmes & Projects

Our expert consultants can provide you with support and guidance across a wide range of services and projects.

Cybersecurity and Vetting Services

Our expert consultants can provide a range of support services and training tailored to meet your requirements.

NCSC CAF

The National Cybersecurity Centre (NCSC) Cyber Assessment Framework (CAF) is the UK's recognised standard for assessing and improving cyber resilience across Critical National Infrastructure (CNI), public sector organisations, and other essential services. Our CAF Compliance Service ensures your organisation aligns with this national framework, strengthening your defensive, detection, and response capabilities.

What is the NCSC CAF?

The CAF is a structured approach to assessing and improving cybersecurity maturity across organisations that support the UK's essential services.

It is structured around four key objectives and 14 security principles, covering:

- Managing Security Risk – Governance, risk management, asset protection, and supply chain security.
- Protecting Against Cyber Attacks – Access control, data security, system security, and network resilience.
- Detecting Cyber Security Events – Security monitoring and proactive threat discovery.
- Minimising the Impact of Cyber Incidents – Incident response, recovery planning, and lessons learned.

Organisations aligning with the CAF framework enhance their ability to defend against cyber threats, reduce disruption risks, and comply with UK security standards.

Why It Matters To You:

- **Ensure Compliance with UK Cyber Security Requirements** – Align with the NCSC Cyber Strategy.
- **Strengthen Cyber Resilience** – Secure essential services against cyber threats and attacks.
- **Prepare for Cyber Oversight Body Assessments** – Demonstrate security governance and risk management maturity.
- **Improve Incident Response & Recovery** – Minimise operational downtime during cyber incidents.
- **Reduce Regulatory & Financial Risk** – Avoid penalties and demonstrate proactive risk mitigation.

GOVASSURE ASSESSMENT

Cyber resilience is critical for government organisations and Critical National Infrastructure (CNI). Our GovAssure Assessment Service provides an independent, expert-led assurance review of your Cyber Assessment Framework (CAF) self-assessment, ensuring accuracy, compliance, and a clear path for improvement.

What is GovAssure?

GovAssure is the UK government's cybersecurity assurance framework, developed by the Government Security Group (GSG) and the National Cybersecurity Centre (NCSC) to strengthen government cyber resilience.

The GovAssure framework assesses critical government systems at OFFICIAL classification and applies to government sector CNI. Organisations must self-assess their security maturity against one of two target CAF profiles:

- **Baseline** – For standard government operations.
- **Enhanced** – For higher-risk systems and functions.

Our GovAssure Stage 4 Assurance Review delivers an independent assessment to verify the accuracy of self-assessment findings, ensuring compliance and providing evidence-based insights for security improvements.

The GovAssure five-stage process includes:

- Understanding organisational context and services.
- Defining in-scope systems and assigning a CAF profile.
- Conducting a self-assessment.
- Performing an independent assurance review (our role).
- Finalising the assessment and developing a Targeted Improvement Plan (TIP).

Amethyst
Making Cyber Secure™

NIS2 DIRECTIVE

The NIS2 Directive introduces enhanced cybersecurity requirements for organisations supporting critical infrastructure across the European Union. Non-compliance can result in significant financial penalties of up to €10 million or 2% of annual turnover for essential entities. Our NIS2 Compliance Service ensures your organisation meets regulatory obligations while strengthening your cybersecurity posture.

What is the NIS2 Directive?

The Network and Information Security (NIS2) Directive is an EU-wide cybersecurity regulation designed to enhance the security of essential and important entities.

Organisations that must comply include those that:

- Operate in the EU and provide critical infrastructure services.
- Employ 50+ employees or generate over €10 million in revenue.
- Operate within 17 key sectors, including energy, transport, healthcare, finance, digital services, and government agencies.
- The UK's Cybersecurity and Resilience Bill is expected to align with NIS2, making compliance essential for UK organisations operating in European markets.

How It Works

We deliver comprehensive, risk-based cloud security solutions to strengthen your cloud infrastructure. We provide a structured approach to achieving and maintaining NIS2 compliance.

Amethyst
Making Cyber Secure™

SECURE BY DESIGN

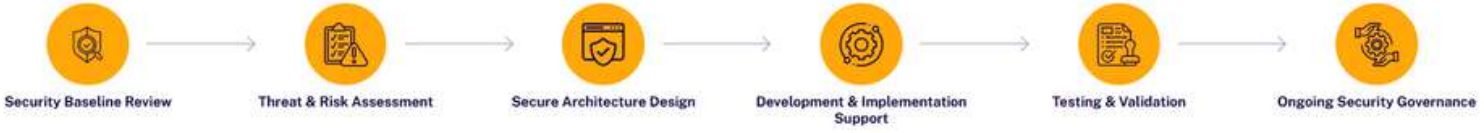
Cyber threats are evolving, and security must be an integral part of your systems from the start. Our Secure by Design service helps organisations embed security into every phase of development, ensuring robust protection and compliance from day one.

What is Secure by Design?
Secure by Design is a proactive approach that integrates cybersecurity principles into the entire development lifecycle. It minimises vulnerabilities, strengthens resilience, and ensures compliance with government security standards.

Why It Matters To You:

- **Proactive Risk Management** – Identify and mitigate risks before they emerge.
- **Regulatory Compliance** – Align with government security frameworks.
- **Default Security** – Ensure systems are secure by default.
- **Reduced Operational Disruptions** – Prevent costly security failures.

Amethyst proactively integrate cybersecurity principles in your development lifecycle:



Why Choose Us:

- Deep expertise in Secure by Design frameworks.
- Established relationships with government and regulatory bodies.
- Customised guidance tailored to your organisation's needs.
- Proven track record of securing mission-critical systems.

Amethyst
Making Cyber Secure™

CYBERSECURITY RISK MANAGEMENT

Understanding and managing cyber risks is critical to protecting your business, operations, and supply chain. Our Cybersecurity Risk Management Service provides expert guidance, helping you identify vulnerabilities, implement security controls, and maintain compliance - ensuring your organisation is resilient against cyber threats.

What is Cybersecurity Risk Management?

Cybersecurity Risk Management is the process of identifying, assessing, and mitigating risks to your IT systems, people, processes, and technology. A strong risk management strategy helps businesses:

- Reduce the likelihood and impact of cyber incidents.
- Ensure compliance with legal, regulatory, and industry standards.
- Protect operations from disruption caused by cyber threats.
- Strengthen supply chain security and vendor risk management.
- Align cybersecurity investments with business objectives.

Our service ensures that security controls are effectively implemented, enabling businesses to meet compliance requirements such as ISO 27001, Cyber Essentials, IASME, and government frameworks like Secure by Design.

Why It Matters To You:

Make Informed Decisions – Understand your cyber risk exposure with expert analysis.

Minimise Financial & Operational Impact – Reduce the risk of costly cyber incidents.

Achieve Compliance & Regulatory Assurance – Meet industry security standards.

Improve Resilience – Ensure business continuity before, during, and after cyber events.

Demonstrate Security Commitment – Build trust with customers and stakeholders.

SUPPLIER ASSURANCE

Your supply chain is only as strong as its weakest link. Our Supplier Assurance service helps you assess, manage, and mitigate security risks across your third-party vendors - ensuring compliance, trust, and resilience.

What is Supply Chain Security Assurance?

What is Supply Chain Security Assurance Supplier assurance is a structured approach to evaluating and managing cybersecurity risks within your supply chain. It ensures that third-party vendors comply with security policies, reducing vulnerabilities and strengthening overall business resilience.

Why It Matters To You:

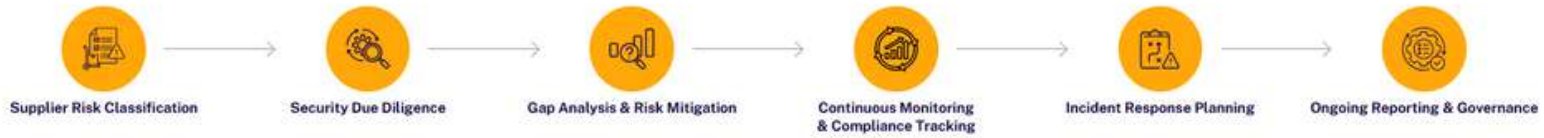
Risk Mitigation – Identify vulnerabilities before they become threats.

Regulatory Compliance – Meet industry and government security standards.

Supplier Accountability – Ensure vendors adhere to security commitments.

Operational Resilience – Reduce disruptions and maintain business continuity.

We provide a structured approach to strengthen the security in your supply chain:



- Trusted by government and enterprise clients to secure critical supply chains.
- Experienced cybersecurity professionals with expertise in supplier risk management.
- Knowledge of industry frameworks such as ISO 27001, NIST, and CIS controls.

Amethyst
Making Cyber Secure™

SECURITY ARCHITECTURE AND DESIGN

In today's rapidly evolving digital landscape, ensuring the security of your IT infrastructure, data, and applications is more critical than ever. Our Security Architecture and Design Service provides expert-led security frameworks and best-practice strategies, ensuring robust protection against cyber threats, data breaches, and compliance risks.

What is Security Architecture & Design?

Security Architecture and Design form the blueprint for an organisation's cybersecurity framework, integrating security into every layer of your IT infrastructure to ensure resilience against current and emerging cyber threats. This involves:

- Security Architecture – Defining the structure, components, and guidelines that protect information systems.
- Security Design – Developing detailed security measures and ensuring they are effectively implemented and maintained.

Our approach follows globally recognised security frameworks, including:

- NIST Cybersecurity Framework (CSF)
- NCSC Cyber Assessment Framework (CAF)
- ISO/IEC 27001
- Secure by Design & Zero Trust Architectures

We design secure network architectures, application security controls, data protection measures, and access management frameworks to meet the highest security standards.

How It Works

Amethyst
Making Cyber Secure™

DATA PROTECTION AND GDPR COMPLIANCE

In today's digital world, data protection is not just a regulatory requirement - it's a business imperative. Our Data Protection and GDPR Compliance Service helps organisations build a resilient data protection framework, ensuring compliance while fostering trust with customers and stakeholders.

What is Data Protection and GDPR Compliance?

Data protection involves safeguarding personal and sensitive information from unauthorised access, loss, or misuse. The General Data Protection Regulation (GDPR) — incorporated into the UK Data Protection Act (2018) — sets strict guidelines on how businesses must handle personal data.

Failure to comply can result in severe financial penalties and reputational damage. Organisations must adhere to key principles such as:

- Transparency & Accountability – Ensuring clear policies on data collection and usage.
- Data Minimisation – Collecting only the necessary information for business purposes.
- Security & Confidentiality – Implementing measures to protect data from breaches.

Why It Matters To You:

Avoid Hefty Fines & Legal Risks – Stay compliant with GDPR, UK DPA (2018), and industry standards.

Strengthen Customer Trust – Demonstrate your commitment to protecting personal information.

Reduce Risk of Data Breaches – Implement robust security controls to prevent data leaks.

Improve Business Efficiency – Streamline data processing, storage, and security frameworks.

Future-Proof Compliance – Stay ahead of regulatory changes and emerging risks.

Amethyst
Making Cyber Secure™

CLOUD SECURITY AS A SERVICE

Whether you're migrating to the cloud for the first time or enhancing existing cloud security, we ensure every step of your cloud journey is secure. Our Cloud Security as a Service provides tailored solutions to help organisations protect cloud environments, mitigate risks, and achieve compliance with industry-leading security standards.

What is Cloud Security as a Service?

Cloud security is essential for protecting data, applications, and workloads across public, private, and hybrid cloud environments. Our services align with leading security frameworks, including:

- Cloud Security Alliance (CSA)
- Centre for Internet Security (CIS)
- ISO 27001:2022, ISO 27017, ISO 27018
- MITRE ATT&CK Cloud Matrix
- NCSC Cyber Assurance Framework (CAF)

We are also industry leaders in AI security, integrating ISO 42001:2023 Artificial Intelligence Management Systems (AIMS) to enable secure AI adoption in the cloud.

Why It Matters To You:

Prevent Cloud Security Breaches – Secure workloads against cyber threats, misconfigurations, and compliance gaps.

Ensure Regulatory Compliance – Meet standards such as ISO 27001:2022, NCSC CAF, FISMA, CSA, and CIS benchmarks.

Strengthen Cloud Posture – Implement continuous security monitoring and risk management.

Enhance Cloud Migration Security – Ensure safe, compliant cloud adoption without business disruption.

Leverage Secure AI & Automation – Safely integrate AI-driven security and cloud automation solutions.

STRATEGY AND POLICY DEVELOPMENT

Cyber threats are constantly evolving, making a clear cybersecurity strategy and enforceable policies is essential for business resilience. Our Cybersecurity Strategy and Policy Development Service helps organisations design and implement robust, practical, and compliance-aligned strategies tailored to their unique risks and regulatory environment.

What is Cybersecurity Strategy and Policy Development?

Cybersecurity strategy and policy development is about building a structured, long-term approach to protecting your organisation against threats. This involves:

- Developing a clear cybersecurity strategy that aligns with industry and government best practices.
- Creating enforceable policies to govern access control, incident response, data security, and regulatory compliance.
- Aligning with global and national frameworks such as ISO 27001, NCSC Cyber Assessment Framework (CAF), GDPR, and the Security Policy Framework (SPF).
- Embedding best practices from the NCSC 10 Steps to Cybersecurity to strengthen resilience.

Why It Matters To You:

Stronger Security Governance – Establish a structured, organisation-wide approach to cybersecurity.

Regulatory & Compliance Alignment – Meet industry and government security requirements (MOD, HMG, ISO 27001, GDPR).

Future-Proofed Security – Adapt to evolving threats and emerging risks.

Operational Resilience – Ensure continuity of operations with proactive risk management.

Clear, Actionable Policies – Provide employees with practical, enforceable security guidelines.

A strong cybersecurity strategy ensures that security is integrated into business operations — not just an afterthought.

Amethyst
Making Cyber Secure™

OPERATIONAL TECHNOLOGY AS A SERVICE

Operational Technology (OT) environments are critical to industrial processes, critical infrastructure, and essential services. Our OT Security as a Service provides risk assessments, architecture design, and governance solutions to ensure continuous, secure, and compliant operations — minimising risks to safety, availability, and business continuity.

Our OT security services follow globally recognised ISA/IEC 62443 cybersecurity standards, ensuring compliance, risk reduction, and secure-by-design architectures.

What is OT Security?

Operational Technology (OT) Security focuses on protecting industrial control systems (ICS), SCADA environments, and connected assets from cyber threats, operational disruptions, and physical security risks.

With the increasing convergence of IT and OT, industrial networks face growing cybersecurity threats, including:

- Ransomware attacks on critical infrastructure.
- Supply chain vulnerabilities impacting OT networks.
- Unpatched legacy systems exposed to external threats.
- Nation-state and targeted cyberattacks on essential services.

Why It Matters To You:

- **Mitigate Cyber Risks in Industrial Systems** – Reduce risks to ICS, SCADA, and industrial networks.
- **Ensure Compliance with OT Security Standards** – Align with ISA/IEC 62443, NCSC CAF, and Secure-by-Design frameworks.
- **Improve Operational Resilience** – Prevent system downtime, safety risks, and production disruptions.
- **Reduce Supply Chain & Insider Threats** – Implement governance frameworks to manage security controls effectively.
- **Protect Critical Infrastructure & Essential Services** – Enhance security for energy, utilities, transportation, and manufacturing sectors.

P3M AS A SERVICE

Effective Project, Programme, and Portfolio Management (P3M) is key to delivering strategic goals, managing resources efficiently, and ensuring business success. Our P3M as a Service provides expert-led project execution, programme leadership, and portfolio optimisation, ensuring your organisation achieves measurable and sustainable results.

Why It Matters To You:

Improve Project Delivery Success – Ensure timely and cost-effective execution.

Maximise Strategic Value – Align projects and programmes with organisational objectives.

Optimise Resources & Reduce Risks – Balance budgets, timelines, and personnel across multiple initiatives.

Strengthen Stakeholder Engagement – Improve communication, collaboration, and transparency.

Enhance Governance & Decision-Making – Implement structured reporting, risk controls, and performance monitoring.

What is P3M?

P3M covers three interconnected disciplines that enable organisations to successfully manage change, align projects with strategy, and optimise resources:

Project Management – Delivering specific objectives within defined timeframes, budgets, and quality standards using structured tools and methodologies.

Programme Management – Coordinating multiple related projects to achieve strategic business outcomes.

Portfolio Management – Managing an organisation's entire suite of projects and programmes, ensuring strategic alignment, risk mitigation, and resource optimisation.

By implementing best-practice methodologies, such as Agile, APM, MSP, and PRINCE2, our P3M solutions drive efficiency, stakeholder engagement, and long-term value creation.

Amethyst
Making Cyber Secure™

CISO AS A SERVICE

Navigating cybersecurity risks and compliance requirements can be overwhelming. Our CISO as a Service provides you with an experienced Chief Information Security Officer (CISO) who will develop and lead your cybersecurity strategy - without the cost of a full-time executive.

What is CISO as a Service?

CISO as a Service delivers flexible, high-level security leadership tailored to your business needs. Our experts work alongside your team to strengthen security, manage risks, and ensure compliance with government and industry standards.

Why It Matters To You:

- **Strategic Security Leadership** – Align cybersecurity with business goals.
- **Regulatory Compliance** – Meet industry security requirements efficiently.
- **Cost-Effective** – Get executive-level expertise without full-time overhead.
- **Risk Reduction** – Strengthen your resilience against cyber threats.

Our CISO service will develop and lead your cybersecurity strategy:

Security Maturity Assessment → Strategy Development → Implementation & Governance → Incident Response & Threat Management → Compliance & Audit Readiness

- Experienced consultants with deep industry knowledge.
- Custom security strategies aligned with your business objectives.
- Strong relationships with regulatory bodies to streamline compliance.
- Proven success in delivering security leadership to government and private sectors.

Amethyst
Making Cyber Secure™

SECURITY CLEARANCE MANAGEMENT

When working on UK Government and defence contracts, managing National Security Vetting (NSV) requirements is critical to ensuring compliance, security, and operational readiness. Our Security Clearance Management Service provides expert-led support in obtaining, managing, and maintaining clearances, ensuring seamless access to classified material and government assets.

What is Security Clearance Management?

Security clearance is a requirement for individuals needing access to classified government information. The clearance process involves comprehensive background checks and, in some cases, detailed vetting procedures.

We provide guidance and management across key clearance levels, including:

- **Baseline Personnel Security Standard (BPSS)** – The minimum clearance required for access to government assets and systems.
- **Security Check (SC)** – A higher-level clearance for individuals requiring long-term, frequent access to SECRET materials.
- **Developed Vetting (DV)** – The highest level of security clearance, required for access to TOP SECRET information.

Our service supports both individuals and organisations, ensuring that all vetting requirements are met, managed, and maintained efficiently.

Why It Matters To You:

- **Ensure Compliance with Government Security Requirements** – Meet MOD, HMG, and NSV guidelines.
- **Access Government & Defence Contracts** – Maintain eligibility for classified projects and secure government roles.
- **Manage Security Clearances Efficiently** – Streamline application, approval, and ongoing clearance management.
- **Minimise Delays & Disruptions** – Reduce risk of expired clearances affecting contract performance.
- **Support Individuals & Organisations** – Provide expert oversight of clearance renewals, audits, and compliance.

CYBERSECURITY TRAINING

Your employees are your first line of defence against cyber threats. Our Cybersecurity Training equips your team with the knowledge and skills to recognise, prevent, and respond to cyber risks — ensuring your organisation stays secure and compliant.

What is Cybersecurity Training?

Cybersecurity training is essential for businesses of all sizes. With cyber threats evolving rapidly, human error remains the leading cause of security breaches. Our training programs help organisations:

- **Reduce Risk** – Employees learn to identify and prevent cyber threats such as phishing, ransomware, and insider attacks.
- **Enhance Data Protection** – Staff gain the skills to securely handle sensitive data, minimising exposure to breaches.
- **Meet Compliance Requirements** – Many industries require regular cybersecurity training to comply with GDPR, ISO 27001, PCI DSS, and other regulations.
- **Strengthen Organisational Security** – A trained workforce acts as a proactive defence against cyber threats.
- **Promote a Security-First Culture** – Encourage secure behaviour in daily operations and decision-making.
- **Reduce Financial Losses** – Prevent costly disruptions, ransom payments, or data recovery expenses.

Investing in cybersecurity training empowers your workforce to act as an active defence against cyber threats.

Core Training Courses Available:

- **Government Cybersecurity** – Training designed for public sector teams handling national infrastructure and sensitive data.
- **Secure by Design** – Develop a security-first approach in software development and system design.
- **Data Protection & GDPR** – Ensure compliance with data protection laws while protecting customer and business information.
- **Supplier Assurance** – Learn how to assess, manage, and secure third-party risks in the supply chain.

Amethyst
Making Cyber Secure™

PENETRATION TESTING AND IT HEALTHCHECK

Cyber threats are constantly evolving, and proactively identifying vulnerabilities is essential for maintaining a secure IT environment. Our Penetration Testing and IT Health Check Services help organisations detect weaknesses, assess risks, and enhance their security posture before attackers can exploit them.

What Are Penetration Testing & IT Health Checks?

We offer a comprehensive suite of security assessments designed to identify vulnerabilities and strengthen IT infrastructure.

- Vulnerability Assessment – A detailed security analysis of your IT systems using advanced scanning tools and methodologies to detect weaknesses such as outdated software, misconfigurations, and unpatched vulnerabilities.
- IT Health Check (ITHC) – A holistic security and performance evaluation of your organisation's IT infrastructure. This includes a vulnerability assessment alongside an efficiency review to identify potential risks and operational inefficiencies.
- Penetration Testing (Pen Testing) – A simulated cyberattack conducted by expert testers to uncover security gaps, misconfigurations, and potential weaknesses before malicious hackers can exploit them.

Our security assessments align with industry best practices, including NCSC CHECK, CREST, and OWASP testing methodologies.

Why It Matters To You:

- **Identify Security Weaknesses** – Find and fix vulnerabilities before attackers can exploit them.
- **Ensure Compliance & Risk Management** – Meet requirements for Cyber Essentials, ISO 27001, GDPR, and regulatory audits.
- **Enhance IT Performance & Security** – Gain clear insights into system health, security gaps, and improvement strategies.
- **Prevent Costly Data Breaches & Downtime** – Minimise financial and reputational damage by strengthening security controls.

OUR COMMITMENT TO EXCELLENCE

Amethyst's commitment to excellence is reflected in the numerous cybersecurity and quality accreditations / certifications we have achieved and maintain, our wide-ranging professional memberships, and our dedication to maintaining the highest standards in every aspect of our business.

The company certifications, accreditations and memberships demonstrate our commitment to deliver high quality, professional, trusted and best in class services to our customers. As a company that depends on the currency of its knowledge and skills, we continually invest in our consultancy team and strive to continually improve.

REACH OUT TO OUR EXPERT TEAM TODAY TO DISCUSS HOW WE CAN HELP PROTECT YOUR BUSINESS WITH TAILORED CYBERSECURITY SOLUTIONS.

sales@amethystrisk.com