

**Protect.
Empower.
Transform.**

Service Overview

SysGroup Cyber Consulting provides professional cybersecurity advisory and consulting services to help organisations assess, improve, and maintain their cybersecurity posture. The service includes cyber risk assessment, security strategy, assurance, compliance readiness, and incident preparedness.

The service is designed for UK SMEs, mid-market organisations, and public and private sector bodies, including those operating in regulated sectors such as finance, healthcare, legal, and SaaS. It addresses common challenges such as limited visibility of cyber risks, difficulty meeting regulatory and standards requirements (for example GDPR or ISO 27001), over-reliance on checklist-based security approaches, poor preparedness for incidents or audits, and limited in-house cybersecurity expertise.

Services are delivered by experienced consultants on a remote, on-site, or hybrid basis. The service does not include a SaaS platform and focuses on practical, outcome-driven recommendations aligned to business and regulatory needs.

Executive Summary

02

SysGroup delivers outcome-driven, enterprise-grade cybersecurity designed to strengthen resilience, reduce operational risk, and enable organisations to operate with confidence. The service combines strategic advisory, advanced technical expertise, and proactive threat defence to provide a holistic, modern, and scalable security approach aligned to today's threat landscape.

Services are delivered by experienced consultants with backgrounds from leading professional services firms and government and defence organisations, supported by certified expertise including CREST, CISSP, and ISO Lead Auditor credentials. Engagements focus on measurable, practical outputs such as prioritised action plans, remediation runbooks, dashboards, maturity scorecards, evidence packs, and clear audit roadmaps.

SysGroup differentiates through outcome-based delivery, rapid mobilisation, hands-on remediation support, and risk-reversal guarantees to ensure findings are actionable and valuable. The service is designed to deliver enterprise-grade security outcomes without unnecessary overhead and is supported by partnered

The service provides an improved understanding of cyber risk and priorities, supported by clear remediation and improvement roadmaps. It increases audit and compliance readiness, reduces the likelihood and impact of cyber incidents, and provides access to specialist cyber expertise without the need for long-term staffing commitments.

Service Methodology and Standards

SysGroup's methodology blends industry-recognised frameworks with practical, business-aligned security delivery. This includes ISO 27001:2022, NIST Cybersecurity Framework, CIS Controls and Benchmarks, CREST and OWASP methodologies, CVSS and KEV/EPSS for vulnerability prioritisation, and sector-specific standards such as GDPR, DPA, PCI DSS and NIS2.

Cyber Maturity Assessments follow ISO 27001 and Annex A control structure, with clear maturity scoring and evidence requirements. Penetration testing follows CREST standards with manual exploitation aligned to OWASP where relevant. Threat modelling, cyber strategy and governance activities draw on NIST and CIS frameworks.

SysGroup goes beyond traditional consultancy approaches by incorporating business impact into every finding, using kill-chain narratives, asset criticality, attack-path modelling, and prioritised remediation. This ensures that recommendations translate directly into improved resilience rather than theoretical compliance.

Our Core Service Portfolio

Our portfolio spans the full cybersecurity lifecycle. From strategy and governance to hands-on technical testing, 24/7 operations, and incident response. Each service is engineered to be clear, measurable, and business-aligned, ensuring security becomes an enabler rather than a barrier.

1. Governance, Risk & Compliance (GRC)

Provides strategic oversight and assurance across governance, risk, and regulatory requirements to strengthen organisational resilience.

Service Outcomes:

- Clear, risk-based decision-making
- Strong governance and policy alignment
- Demonstrable regulatory readiness
- Controlled and measurable supply-chain security

Includes: Risk Management, Threat Modelling, Policy & Standards, Strategy & Maturity Assessments, Compliance Advisory, Third-Party Risk Management.

2. Training & Awareness

Delivers targeted, high-impact training to strengthen security culture and reduce human-factor risk.

Includes: Post-incident awareness and refresher training programmes.

3. Data Protection

Ensures sensitive data is safeguarded through proactive prevention and continuous oversight.

Includes: Data Loss Prevention (DLP) management and operational governance.

4. Security Operations

Maintains secure, resilient technology environments with strong architectural foundations and best-practice configuration.

Service Outcomes:

- Robust security baselines
- Reduced attack surface
- Consistent security across cloud and on-premises services

Includes: Security Architecture, Hardening, Secure Configuration, Cloud Security Posture Management, Identity & Access Management.

5. Security Testing

Provides independent validation of security controls through structured testing, simulation, and secure development assurance.

Service Outcomes:

- Verified control effectiveness
- Improved response readiness
- Early detection of systemic weaknesses

Includes: Penetration Testing & Validation, Tabletop & War-Gaming Exercises, Secure Code Reviews, Breach & Attack Simulation.

6. **Business Continuity & Security Recovery**

Strengthens organisational resilience and ensures critical security functions can operate during and after a disruption.

Includes: BC/DR planning for the security organisation, backup and recovery testing.

7. **Managed Detection & Response (MDR)**

Delivers continuous monitoring, threat detection, intelligence, and response support to protect against advanced threats.

Service Outcomes:

- Faster detection and containment
- Enhanced visibility across the estate
- Intelligence-led defence

Includes: Threat Hunting, Log Correlation, SOC Support (24/7), Threat Intelligence, Insider Threat Monitoring, SIEM Tuning, Dark Web Monitoring, Phishing & Fraud Detection.

8. **Incident Investigation & Digital Forensics**

Provides rapid incident response, forensic investigation, and post-incident assurance to minimise impact and prevent recurrence.

Service Outcomes:

- Rapid containment and eradication
- Clear root-cause analysis
- Strengthened controls after incidents

Includes: Incident Investigation & Remediation, Incident Response Retainer, Digital Forensics & Readiness Assessment.

Services are provided on a time and materials basis or as fixed-scope engagements, with pricing defined in an agreed Statement of Work prior to service commencement.

Any variations to scope or effort are subject to mutual agreement. Additional scope charged at standard rates, travel, subsistence, and third-party costs charged at cost.

Onboarding & Offboarding

Engagement begins with the agreement of a Statement of Work that defines the scope, objectives, timelines, deliverables and roles and responsibilities for the engagement. An initial onboarding meeting is held to confirm requirements, agree communication and governance arrangements and establish access, information sharing and reporting processes as required for service delivery.

Offboarding is conducted in a controlled and orderly manner at the end of the engagement or upon termination. This includes the completion of agreed deliverables, handover of outputs and the secure return or deletion of customer information in line with contractual obligations and applicable data protection requirements.

SysGroup provides qualified cyber security consultants, delivers services with reasonable care, skill and diligence, and produces reports, findings, and documentation.

Customers provide access to relevant systems, data and personnel, ensure timely responses and approvals and have the authority to share data or grant access.

Below is a representative sample of industries that trust SysGroup to enhance, manage, and secure their digital environments. These partnerships reflect our proven ability to deliver reliable, high-quality solutions tailored to each client's needs. By combining industry expertise with a customer-first approach, we help organisations strengthen their IT foundations and operate with confidence.

Finance

The financial services industry is one of the most heavily regulated and targeted by cybercriminals. High-value transactions, sensitive data, and reliance on global digital infrastructure create a complex risk landscape.

Insurance

Insurance organisations process extensive personal and financial data, making privacy, fraud prevention, and operational continuity essential.

Legal & Professional Services

Law firms handle privileged, confidential and often highly sensitive corporate information. They are increasingly targeted by ransomware groups.

Technology, Cyber, Digital

Tech organisations often operate complex, high-velocity environments requiring robust security to maintain trust and protect intellectual property.

Consulting & Business Services

Consultancies manage client data across many industries and often operate distributed teams. Confidentiality and integrity are critical.

Manufacturing & Industrial

Manufacturers often face combined IT and OT (Operational Technology) risks. Downtime is costly and safety concerns can be significant.

Transport

Transport depends on real-time systems, operational safety, and logistics networks, often intertwined with legacy IT.

Energy & Infrastructure

Critical infrastructure faces geopolitical threats, nation-state attacks, and strict regulatory expectations. Reliability and resilience are paramount.

Retail

Retail deals heavily with customer data, payment systems, and high-traffic digital platforms. Brand reputation is highly sensitive to breaches.

SysGroup responsibilities

- Deliver services with reasonable care, skill, and diligence
- Maintain confidentiality
- Comply with applicable laws

Customer responsibilities

- Provide accurate information and access
- Pay fees in accordance with the agreement
- Ensure lawful processing of data

SysGroup's cybersecurity team combines strategic thinkers, technical specialists, and former defence personnel. They are all united by a commitment to excellence, precision, and client impact.



Chris Wilkinson — Head of Cybersecurity

Chris is an accomplished cybersecurity leader with deep expertise across Governance, Risk, Compliance, Incident Response, Audit, and Security Strategy. With senior roles at PwC and KPMG, he has delivered major security transformations within Financial Services, Telcos, Government departments, and national infrastructure. An ex-RAF officer, Chris brings disciplined leadership and a mission-driven approach to every engagement.



James Henry — Cyber Consulting Director

James is a senior advisor specialising in Governance, Risk, Compliance, Incident Response, and Audit. His experience spans Ernst & Young, Finmeccanica, Leonardo, defence, law enforcement, health, space, international security, financial services, and UK Government departments. He is known for his ability to guide complex organisations through high-stakes risk and resilience challenges.



Laura Greenwood — Cyber Consulting Associate Director

Laura is a Third-Party Risk Management specialist with a background in financial services and fraud investigation. Her analytical approach and deep understanding of supply-chain security help organisations manage vendor ecosystems with confidence and clarity.



Alan Lim — Cyber Consulting Associate Director

Alan is an expert in penetration testing, audit, and offensive security across multiple sectors. He has led red-team engagements, adversary simulations, and technical assurance programmes for high-risk and regulated organisations, delivering actionable insights that materially strengthen security posture.



Ryan King — Cyber Consulting Associate Director

Ryan leads SysGroup's Security Architecture capability with experience from KPMG and across diverse industry verticals. His background in manufacturing and operational technology security, combined with prior expertise as a penetration tester, brings a unique blend of offensive and defensive knowledge. A former French Foreign Legionnaire, Ryan brings exceptional discipline, adaptability, and operational rigour.