LOGIQ

INNOVATE. COLLABORATE. DELIVER.

CLOUD SUPPORT
SERVICE DEFINITION

RM1557.15 | Date: 30th January 2026 | Version: 1.0

Making Security The Foundation Of Every Business

LOGIQ

Company Overview

Logiq is a NCSC-assured and ISO 27001 certified cyber security consultancy and secure solutions provider focused on safeguarding critical organisational data.

NCSC assured for Risk Management, Security Architecture and Audit and Review, we're experts in cloud services and data protection, specialising in cost effective, cyber secure solutions for highly regulated sectors and clients including the MOD, Central Government, Critical National Infrastructure (CNI) and the wider public sector.

We have significant experience in designing secure networks specifically to meet the security standard required to hold HMG sensitive information and are trusted by the MOD to support Information Assurance and cyber defence across multiple mission critical systems at the highest classifications.

Through a modern, forward-thinking approach that meets the complex security needs of our clients, we deliver systems that significantly improve cyber resilience and mitigate risk, enabling us to make security the foundation of every business.

Our security consultancy expertise spans:

- Systems / Security Engineering
- Secure by Design
- Solution Architecture
- System Design and Implementation
- Technical and Agile Project Management
- Cloud Architecture and Development
- Risk Management
- Cyber Assessment Framework (CAF) / GovAssure
- OT / ICS
- Specialising in Defence and Regulated Sectors

Secure Solutions

- DISX® - secure, scalable data collaboration and communications
- Secure Managed Services
- Microsoft 365 productivity suite
- Secure cloud proof of concept systems
- Secure app hosting for business critical software

All our services are delivered or overseen by Developed Vetting (DV) and Security Check (SC) cleared staff, and our cloud architecture solutions adhere to, and are aligned to, HMG and NCSC guidelines and policies.

Utilising UK sovereign cloud services, our solutions for network assurance meet the required standards for both the MOD and Other Government Departments.

Logiq is a Microsoft Solutions Partner.
Security and Modern Workplace

Microsoft Solutions Partner

bsi ISO/IEC 27001 Information Security Management CERTIFIED

bsi ISO/IEC 20000-1 IT Service Management CERTIFIED

ISO 9001 ISOQAR REGISTERED

Cyber Security and Assurance

Cloud Support

RM1557.15

LOGIQ.CO.UK

Cyber Security
Cyber Security and Assurance

Logiq's Cyber Security experts support multiple clients, and design secure solutions supporting a range of cloud and on-premise architectures. Delivering Defence Digital Cyber Programmes, Information Security, Enterprise Architecture (MODAF, TOGAF), RMADS, Risk Assessments, Security Design, Cloud Security Architecture, System Design, Project Management, Agile Coaching, Professionalisation, Transformation, Cloud Migration.

Features

- Developed Vetting (DV) and Security Check (SC) cleared staff
- Full security risk management
- Cyber Security Policies and Processes
- Cloud and system assessments to identify threats and vulnerabilities
- Identify security risks and prepare mitigation plans
- Secure by Design (SbD) implementation
- Cyber Project and Programme Management and Approvals
- Agile Project Management
- Agile Coaching supporting cyber projects

Benefits

- Adhere and aligned to HMG and NCSC guidelines and policies
- Compliance and understanding of the General Data Protection Regulation (GDPR)
- Provide transfer of latest industry knowledge
- Professionalisation of delivery workforce
- Service delivered by industry recognised cyber security experts

Audit and Review
Cyber Security and Assurance

Delivering independent, tailored cyber and information security audits that assess risks, governance, threats, and vulnerabilities. Our qualified specialists apply international and UK HMG best practice, NIS, ISO 27001, and ISO 62443 frameworks to enhance resilience, reduce business risk, assure compliance, and support preparation for formal security certification.

Features

- Qualified professionals providing independent security compliance audits
- Bespoke approach to deliver optimum outcomes
- Review and outline of threat and vulnerability landscape
- Compliance or risk based audits
- Bespoke approach for cyber and information security audits
- Security governance review, ISMS documentation processes and procedures
- UK HMG frameworks and best practice (SPF, CAF, Cyber Essentials)
- National Cyber Security Strategy
- NIS regulations and ISO 27001

Benefits

- Bespoke delivery to meet business requirements
- Improve overall cyber resilience and cyber security posture
- Security compliance audits
- Impartial assessments aligned with security compliance
- Reduces overall business risk landscape
- Qualitative and quantitative audit methods
- Preparation for formal security certification

Risk Management
Cyber Security and Assurance

Tailored NCSC Assured Risk Management services using a range of techniques appropriate to the technology or organisation, including complex and novel problems. Includes defining risk appetite, risk assessment, mitigation, identifying suitable controls, strengthening security architecture, and applying enterprise-wide methodologies that enhance resilience and support cyber security improvements across organisations.

Features

- Tailored solutions addressing unique security challenges
- Early security adoption in project lifecycle
- Qualified Information Assurance & Risk Assessors CISM, CITP, ISO27001
- Cyber security policy, standards, procedures and compliance
- Risk Management Frameworks – Cyber Assessment Framework (CAF)
- Cloud security assessments
- Information Assurance policies and procedures
- Cyber Security as a Service (CSaaS)
- Cyber Security Strategy incorporating NIST CIS Controls

Benefits

- Aligning security approach with risk appetite
- Security Architecture enhancement
- Strengthened architecture defence compliant with regulatory requirements
- Embedding resilient security posture
- Agile approach to delivery
- Enterprise wide Risk Management methodologies
- Cloud solutions

Security Architecture
Cyber Security and Assurance

A security architecture service that translates business requirements into secure, actionable designs. Delivered in line with NCSC Assured principles, it develops cloud-ready architectures, integrates security into DevOps and containerised platforms, and supports complex digital environments. The service strengthens enterprise security through clear architectural direction across defence, CNI and government systems.

Features

- NCSC-assured security architecture design services
- Translation of business requirements into secure architectures
- Cloud-ready architecture for complex digital environments
- Secure DevOps and container architecture design
- Enterprise-scale architecture across defence and CNI contexts

Benefits

- Architecture Framework aligned - TOGAF, MODAF, DODAF, SABSA
- Clear security architecture blueprints and roadmaps
- Improved enterprise security posture and resilience
- Consistent alignment with NCSC and NIST principles
- Reduced design risk across complex environments
- Secure foundations for cloud and digital transformationCyber Essentials Plus certified organisation
- Cyber Assessor certified experts
-

Cyber Assessment Framework (CAF)

Cyber Security and Assurance

Delivery of CAF aligned risk management, internal audits, and gap analysis across all principles to define scope, map evidence, integrate existing standards, and support GovAssure readiness and audit. Our approach strengthens cyber maturity, streamlines compliance, improves assurance confidence, and provides practical remediation for sustained, security improvement.

Features
• CAF-aligned risk management design and implementation
• Internal CAF audits and structured gap analysis
• Support across all CAF Principles, COs and IGPs
• Scope definition and profile selection
• Evidence identification and assurance mapping
• Integration of existing standards and certifications
• GovAssure Independent Assurance Reviews
• Targeted improvement and remediation planning

Benefits
• Clear understanding of cyber risk maturity
• Proportionate, defensible security controls
• Reduced duplication across frameworks
• Greater confidence in assessment outcomes
• Improved readiness for assurance reviews
• Practical, implementable recommendations
• Alignment with government expectations
• Sustained improvement beyond point-in-time audits

GovAssure

Cyber Security and Assurance

Meeting the standard for GovAssure, we are recognised as an NCSC Assured Consultancy for Risk Management and Security Architecture, validating our cyber expertise, reflected throughout our service offerings. Understanding that GovAssure aims to strengthen cyber resilience throughout Government IT infrastructure, we align our services with NCSC's Cyber Assessment Framework (CAF), assessing risk management, gaps, incident response and access control, thereby supporting the principles of GovAssure.

Features
• Effective validation of risk assessment against the Cyber Assessment Framework
• Ability to assist with implementation of the Cyber Assessment Framework
• Linkage of the risk assessment to organisation goals and functions
• Ability to produce tailored Information Assurance Report enabling organisational outcomes
• Post IAR review of targeted improvement plan
• Ability to perform Lessons Identified workshop to enabling process improvements

Benefits
• Enables understanding the risk posture of the department
• Enables action plan to improve the cyber resilience of the department
• Enabling effective risk remediation activity
• Enabling lessons identified to actively improve processes
• Alignment to the Government Cyber Strategy

Secure by Design

Cloud Support

RM1557.15

LOGIQ.CO.UK

Secure by Design
System Delivery and Assurance

A secure-by-design delivery and assurance service supporting government projects meet mandated security principles throughout delivery. It embeds security leadership, risk management and continuous assurance into programmes, supports secure requirements and architecture development, and provides oversight to ensure systems and services meet Secure by Design expectations across cloud and on-prem environments.

Features

- Secure by Design strategy development, enterprise adoption & transformation
- SbD principles and continuous assurance process through implementation
- Delivery Team Security Lead support (including Above Secret systems)
- Risk Management and Assurance / Project Security Management Plan production
- Cyber Security Scoping Appraisals and Security Risk Assessment production
- Secure System / Service Requirements capture (User, Functional, Security)
- Security conscious Business, Enterprise, and Solution Architecture development and design
- Security Architecture development, design, implementation, evaluation, testing, and assurance
- Public and Private Cloud application development, deployment, security assessments, assurance

Benefits

- Service delivered by industry leading cyber security experts
- Assessment Phase and Discovery Phase support
- Detailed understanding of Secure by Design assurance principles and approach
- Government projects delivered meeting Secure by Design principles
- Reduced delivery risk through continuous security assurance
- Clear evidence of compliance with mandated security requirements
- Security embedded throughout project delivery lifecycle
- Increased confidence in system security

Secure by Design
Training

As the leading industry delivery partner for Secure by Design (SbD) training across Government, our SbD experts ensure our clients' organisations are equipped to deliver risk centric designs to meet business objectives, enhance system resilience, reduce cost and comply with regulations.

Features

- Introduction to systems thinking for security
- Understanding of Secure by Design and its benefits
- How to establish what is needed from security
- Guidance for setting of security requirements and assigning controls
- Guidance on using standards and policies
- How to gain and maintain assurance for regulatory bodies
- One to one key stakeholder engagement
- Delivery through workshops, where relevant
- Tools to self-assess risk and attain desired outcomes
- DV and/or SC cleared experts to suit programme classifications

Benefits

- Moves attendees from compliance to design
- Empowers to continually identify and manage risk
- Ensure system and projects are future ready
- Embed culture of security first & throughout
- Seamless integration of Secure by Design principles

Secure by Design
Assessments

Delivery of independent, government-aligned Secure by Design assessments that ensure security has been built in from the outset. Interrogation of architectures, design decisions and delivery plans to present all risks, validate assumptions and provide authoritative, evidence-driven findings that strengthen security, resilience and assurance.

Features

- Developed Vetted (DV) and Security Check (SC) cleared staff
- Government-aligned Secure by Design evaluation
- Early-lifecycle architecture and solution assessment
- Constructive challenge of security and engineering assumptions
- Risk-centred analysis of technical and programmatic dependencies
- Clear, credible evidence suitable for audit, governance and assurance
- Expert recommendations grounded in MOD and cross-government SbD experience
- Identification of systemic, architectural and procedural gaps

Benefits

- Trusted, independent view of design security and resilience
- Earlier detection of risks that typically emerge too late
- Increased predictability of delivery outcomes
- Appropriately informed technical and programme decisions
- Stronger alignment with Government and regulated-sector expectations
- Reduced rework, reduced programme risk, stronger assurance posture
- Evidential basis for strategic, architectural and investment decisions

Secure by Design
Transformation

Delivery of Secure by Design transformation, shifting organisations from a compliance-based security approach, to one that delivers integrated/proactive continual cyber security risk management to enable more secure, trustworthy and resilient systems.

Features

- Transformation from compliance-led to risk-led security
- Integrated cyber security across organisational delivery
- Continuous risk identification and management processes
- Secure-by-design operating models and governance
- Organisational change support for secure transformation

Benefits

- Proactive management of cyber security risk
- Reduced reliance on reactive compliance controls
- More secure and resilient systems
- Improved trust in digital and cloud services
- Sustainable, embedded security practices

Operational Technology (OT)

Cloud Support

RM1557.15

LOGIQ.CO.UK

Operational Technology
Audit and Assurance

Logiq delivers NCSC Assured Independent OT audit aligned to NIS, COMAH, NCSC CAF, ISA/IEC 62443 and NIST 800 82. Validates governance, technical controls, and operational practices across OT systems such as SCADA, DCS, PLC, RTU and IIoT systems, delivering actionable assurance for regulators and board-level risk visibility.

Features

- Identifies systemic weaknesses and vulnerabilities
- Benchmarks against NCSC CAF profiles
- Validates cybersecurity policies, standards, and compliance
- Reviews zones and conduits for secure architecture
- Aligns with GovAssure, NCSC CRA and Competent Authority frameworks
- Comprehensive coverage of SCADA, DCS, PLC, RTU, IIoT
- Risk-based prioritisation of findings
- Supports regulatory and audit readiness

Benefits

- Demonstrates NCSC-assured compliance
- Aligns cyber risk with process safety (COMAH)
- Supports prioritised risk treatment plans
- Supports NCSC CAF contributing outcomes
- Provides assurance on risk decisions
- Improves investment justification for remediation
- Strengthens evidence for regulators and auditors
- Enhances board-level visibility and governance
- Reduces likelihood of operational disruption
- Builds resilience against evolving OT threats

Operational Technology
Business Process Mapping

Mapping business-critical OT processes, dependencies, and data flows to strengthen resilience and support business outcomes. Aligns with NIS, COMAH, and NCSC CAF requirements, linking SCADA/DCS operations to organisational risk management and assurance frameworks for improved continuity and compliance.

Features

- Identifies systemic weaknesses and process gaps
- Delivered by ISA/IEC 62443 certified experts
- Maps critical process dependencies for operational continuity
- Aligns with COMAH safety case requirements
- Improves incident response planning and recovery strategies
- Integrates OT process mapping with business resilience objectives
- Supports governance and assurance cycles
- Provides actionable insights for risk-based decision-making

Benefits

- Demonstrates NCSC-assured compliance alignment
- Supports OG-86 guidance in COMAH regulations
- Informs investment decisions with clear dependency mapping
- Enables defensible risk acceptance and governance
- Supports KPIs and assurance cycles for OT resilience
- Strengthens evidence for regulators and auditors
- Enhances board-level visibility and strategic oversight
- Improves operational continuity and recovery planning
- Reduces risk of cascading failures in OT environments
- Builds resilience against evolving threats and disruptions

Operational Technology
Security Safety Process

Integrated approach combining OT safety and cyber risk management. Applies HAZOP and LOPA supporting IEC 61508/61511 and ISA/IEC 62443 to assess cyber-initiated hazards, strengthen safeguards, and protect people, assets, and production while evidencing COMAH compliance and enhancing business resilience.

Features

- Embeds HAZOP and LOPA into cyber risk assessments
- Aligns with IEC 61508/61511, NIS, COMAH, and NCSC CAF
- Delivered by ISA/IEC 62443 certified experts
- Supports secure segmentation for SIS, BPCS, and OT systems
- Agile methodology enabling business change management
- Prioritises high-consequence scenarios and SIL targets
- Links cyber threats to process hazards and safety functions
- Provides defensible security architecture for safety-critical systems
- Integrates safety and cybersecurity governance frameworks
- Delivers actionable recommendations for risk reduction

Benefits

- Early identification of cyber-safety risks and mitigations
- Embeds security and safety from project inception
- Improves design of safeguards, alarms, and protective logic
- Reduces vulnerabilities and long-term security costs
- Provides audit-ready documentation for regulators and insurers
- Enhances resilience against cyber-initiated process disruptions
- Supports defensible risk acceptance and governance decisions
- Aligns safety integrity levels (SIL) with cyber risk posture
- Builds confidence in operational continuity and safety assurance
- Strengthens regulatory compliance and COMAH safety case evidence

Operational Technology
Incident Response Exercise Service

Structured OT cyber incident response exercises to validate detection, containment, and recovery processes. Aligns with NIS, NCSC CAF, and ISA/IEC 62443 standards, delivering lessons learned to improve policies, resilience, and organisational awareness across OT systems such has SCADA, DCS, PLC, and safety-critical systems

Features

- Simulates realistic OT cyber incidents
- Identifies procedural, technical, and governance gaps
- Delivered by ISA/IEC 62443 certified experts
- Develops and tests OT-specific incident response plans
- Links cyber threats to process hazards and safety functions
- Provides actionable lessons learned and improvement roadmap
- Enhances cross-team coordination and communication
- Integrates findings into policy and resilience strategies
- Aligns with NIS and NCSC CAF risk frameworks
- Supports secure architectures for SIS, BPCS, and SCADA

Benefits

- Improves organisational resilience and readiness for OT cyber incidents
- Strengthens incident response policies and governance frameworks
- Identifies lessons learned to enhance future response capability
- Builds awareness and confidence across operational and leadership teams
- Reduces downtime and operational disruption through proactive planning
- Provides audit-ready evidence for regulators and insurers
- Supports defensible risk acceptance and compliance alignment
- Enhances cross-functional collaboration and decision-making under pressure
- Drives continuous improvement in security posture and safety assurance
- Aligns response capability with business continuity and risk appetite

Operational Technology
Risk Management

Logiq delivers comprehensive OT risk assessments aligned to NIS, COMAH, NCSC CAF, ISA/IEC 62443 and NIST 800 82. This incorporates OT systems such as SCADA, DCS, PLC, RTU and IIoT assets, incorporating protocol-specific threat modelling and consequence-driven analysis to deliver actionable insights and prioritised risk treatment plans.

Features

- Tailored solutions for unique OT security challenges
- Review IT and OT vulnerabilities including remote access
- Delivered by ISA/IEC 62443 certified experts
- Alignment with cybersecurity policies, standards, and compliance requirements
- Risk management using NCSC Cyber Assessment Framework (CAF)
- Supports Information assurance policies and governance
- Secure architecture review of zones and conduits
- Protocol-aware OT threat modelling and attack surface analysis
- Consequence-driven risk evaluation for critical processes
- Identifies credible worst-case scenarios and mitigations

Benefits

- Supports regulatory and audit readiness
- Aligns cyber risk with process safety (COMAH)
- Provides prioritised and actionable risk treatment plans
- NCSC Assured service supporting NCSC CAF risk management outcomes
- Enables defensible risk acceptance decisions
- Improves investment justification for security measures
- Aligns security strategy with organisational risk appetite
- Enhances OT security architecture and resilience
- Strengthens regulatory compliance evidence
- Reduces likelihood of operational disruption

Operational Technology
Secure by Design & Lifecycle Security

Embedding ISA/IEC 62443, NIST 800 82, and NCSC CAF principles across the OT lifecycle from concept to decommissioning, ensuring SCADA, DCS, PLC, RTU, and IIoT systems are secure by design and remain resilient in operation, supporting organisational security programs and regulatory compliance.

Features

- Industry-recognised Secure by Design specialists
- Experience supporting MOD Secure by Design initiatives
- Delivered by ISA/IEC 62443 certified experts
- Embeds ISA/IEC 62443 lifecycle security controls
- Implements Secure by Design frameworks and guidance
- Training and knowledge transfer for internal teams
- Agile methodology supporting business change management
- Secure cloud development and integration
- Governance alignment with NCSC CAF principles
- Continuous security assurance throughout OT lifecycle

Benefits

- Early risk identification and proactive mitigation
- Establishes secure configuration baselines and change control
- Embeds security from project inception
- Enables compliance with Secure by Design policies
- Reduces vulnerabilities and long-term security costs
- Streamlines processes for faster development cycles
- Provides bespoke risk management frameworks
- Strengthens regulatory compliance and audit readiness
- Enhances business resilience and operational continuity
- Improves stakeholder confidence in OT security posture

Operational Technology
Security Architecture

Design and implementation of Operational Technology (OT) security architectures using ISA/IEC 62443 zones and conduits, aligned to NIS, COMAH, and NCSC CAF. Provides secure segmentation and resilience across OT systems such as SCADA, DCS, PLC, RTU, and IIoT environments, supporting risk-based decisions and regulatory compliance.

Features
• Aligns to ISA/IEC 62443 segmentation principles
• Delivered by ISA/IEC 62443 certified experts and TOGAF/ AWS architects
• Integration with DevOps and secure cloud environments
• Defence-experienced cloud and OT security architects
• Enables secure remote access while strengthening resilience
• Clear zone and conduit reference model for OT networks
• Consultancy aligned with IT frameworks (ISO 27001)
• Supports hybrid IT/OT architecture convergence
• Incorporates monitoring and detection capabilities

Benefits
• Provides a security architecture blueprint and roadmap
• Embeds secure design principles across the organisation
• Aligns with NCSC, ISA/IEC 62443, and NIST guidelines
• Delivered by industry-recognised specialists (TOGAF, CISSP, CISM)
• Leverages MODCloud and CNI programme experience
• Cyber Essentials Plus certified organisation and assessor expertise
• Enhances monitoring, detection, and incident response capabilities
• Improves resilience against evolving OT threats
• Supports regulatory compliance and audit readiness
• Strengthens governance and risk management outcomes

Technical Programme Support

Cloud Support

RM1557.15

LOGIQ.CO.UK

Business Analysis
Technical Programme Support

A business analysis service that captures business needs, user requirements and process impacts to support successful change and cloud adoption. It evaluates current operations, defines future-state processes and assesses gaps, enabling informed decisions and clear requirements. The service helps ensure effective solutions, reduced delivery risk and aligned transformation outcomes.

Features
- Analysis of business processes and user needs
- Requirements capture and validation
- Mapping to future architectures and strategies
- Business process modelling and improvement
- Solution evaluation and recommendation
- Impact assessment and gap analysis
- Change planning and stakeholder engagement
- Training and knowledge transfer

Benefits
- Clarity on business needs and priorities
- Reduced ambiguity and delivery risk
- Improved alignment to organisational objectives
- Stronger stakeholder engagement and understanding
- Optimised processes and operational efficiency
- Better decision-making through structured analysis
- Smoother transition to modern cloud services
- Solutions aligned to future-proof architectures

Portfolio, Programme and Project Management
Technical Programme Support

A P3M service providing structured management of complex cloud, ICT and secure programmes. Specialists apply APM, PRINCE2 and Agile practices to coordinate delivery, manage risks and dependencies, and maintain transparent governance. The service helps deliver successful outcomes by ensuring controlled progress from initiation through to benefits realisation.

Features
- Coordination of risks, issues, opportunities and dependencies
- Integration with governance and assurance frameworks
- Blend of Programme, Project and Portfolio specialists
- Expert APM, Agile, Waterfall and hybrid delivery
- Rigourous management to time, cost and quality
- Collaborative open and transparent stakeholder engagement
- Mentoring & coaching
- Delivery planning aligned to organisational objectives
- Transparent reporting of progress and performance
- Continuous optimisation of delivery processes

Benefits
- Greater delivery control across complex programmes
- Improved alignment with strategic business goals
- Reduced risk through proactive management
- Clear visibility of progress and constraints
- Enhanced stakeholder confidence and collaboration
- Streamlined delivery across teams and workstreams
- Stronger assurance throughout the lifecycle
- Better prioritisation and resource use

Systems Engineering
Technical Programme Support

A systems engineering service supporting complex programmes through requirements definition, architectural design and multidisciplinary integration. DV and SC-cleared engineers apply industry standards to model problems and develop secure, scalable solutions. The service helps deliver complex systems-of-systems by guiding technical decisions, managing interdependencies and maintaining engineering coherence across programmes.

Features
- Requirements definition and validation across complex systems
- Architectural design for secure, scalable solutions
- Multidisciplinary engineering integration and coordination
- Technical risk, dependency and interface management
- Alignment with industry standards and governance frameworks
- Evaluation of solution options and trade-offs
- Transition support across the engineering lifecycle

Benefits
- Clear requirements reducing delivery uncertainty
- Coherent technical direction across systems and teams
- Reduced technical risk through early insight
- Better integration of diverse systems and components
- Improved solution quality and long-term sustainability
- Successful delivery of complex systems-of-systems challenges
- Decisions informed by structured technical analysis

Business Intelligence
Technical Programme Support

A business intelligence service that assesses organisational data needs and defines the insights required for effective decision-making. It analyses processes, information flows and performance measures to identify gaps, priorities and opportunities. The service helps organisations understand what intelligence they need and how to exploit it to improve outcomes.

Features
- Assessment of organisational data needs
- Analysis of processes and information flows
- Identification of intelligence gaps and priorities
- Definition of required performance measures
- Mapping of decision-support requirements
- Stakeholder engagement to capture insight needs
- Alignment with business objectives and outcomes
- Recommendations for effective intelligence exploitation

Benefits
- Clear understanding of required business intelligence
- Better alignment between data and decision-making
- Identification of trends, risks and opportunities
- Improved organisational visibility and insight readiness
- Reduced ambiguity around reporting and metrics
- Stronger foundation for future BI development

Data Analytics, Power BI & Apps
Technical Programme Support

A data analytics service enabling organisations to access, model and visualise business-critical information. Using cloud platforms, Power BI and Power Apps, it provides real-time reporting, advanced analysis and structured data governance. The service improves decision-making by transforming complex datasets into meaningful insights and supporting reliable, scalable business intelligence solutions.

Features

- Advanced data analysis and modelling
- Real-time dashboards and visualisations
- Automated dataflows and transformations
- PowerBI and Power Apps development for workflows
- Cloud-based data integration
- Training and capability uplift
- Data governance and security controls

Benefits

- Extracts insights from complex datasets
- Reduces manual reporting effort
- Enables custom workflows and apps
- Provides real-time operational intelligence
- Improves data reliability and trust
- Aligns analytics outputs to business needs

Product Ownership
Technical Programme Support

Product Ownership leadership and support across Discovery, Alpha and Beta phases for complex technical programmes across government organisations. Proficient in a range of techniques, including Scrum, SAFe and Lean, to define product vision, prioritise backlogs, manage risk and deliver secure, outcome-focused solutions aligned to strategic objectives.

Features

- Flexible in our approach to support internal skills and capacity
- Ensuring product backlog is transparent, visible and understood
- Backed by years of hands-on experience within the MOD
- Effective workshop hosting for PI planning, retrospectives or sprint reviews
- Coaching and empowering teams and senior stakeholders
- Customer feedback management
- Leading teams through their digital transformation
- Support with Service Exec Model (SEM), projects to product delivery
- Iterative delivery and continuous improvement focused

Benefits

- Focus on frequent delivery of value
- Deep experience of Discovery, Alpha and Beta phases
- Experienced Product Owners accredited to A-CSPO level
- Representing the needs of all stakeholders
- Specialists in Cyber Security programmes
- Risks effectively identified, managed and included in product backlog
- Experts in Scaled Agile delivery, eg SAFe or LeSS

Agile Delivery
Technical Programme Support

A secure agile delivery service supporting complex digital and transformation programmes. DV-cleared consultants lead agile planning, coordination and technical assurance using SAFe, Scrum, Kanban and Lean practices. The service enables transparent, outcome-focused delivery aligned with organisational objectives, governance requirements and evolving programme priorities.

Features

- Agile delivery management cross multi-team and programme environments
- Technical programme coordination and dependency management
- Backlog prioritisation and delivery planning aligned to business outcomes
- Stakeholder engagement and communication planning
- Risk, issue, and dependency identification and mitigation
- Integration of agile delivery with governance and assurance frameworks
- Reporting on delivery progress, outcomes, and performance
- Continuous improvement and delivery optimisation
- Knowledge transfer and capability uplift for client teams
- Developed Vetting (DV) and Security Check (SC) professionals

Benefits

- Improved delivery confidence across complex technical programmes
- Faster delivery of value through effective agile practices
- Reduced delivery risk through proactive assurance and coordination
- Clear visibility of progress, risks, and dependencies
- Better alignment between technical delivery and business objectives
- Stronger stakeholder trust and engagement
- Increased adaptability to changing priorities and constraints
- Improved quality and readiness at go-live
- Sustainable delivery capability embedded within client teams
- Delivery that balances speed, security, and compliance

Solution Delivery

Cloud Support

RM1557.15

LOGIQ.CO.UK

ServiceNow
Solution Delivery

Logiq provides end-to-end licence, implementation, deployment, upgrade, monitoring & maintenance services for ServiceNow platforms, hosted via ServiceNow's SaaS model or customers' infrastructure, specialising in highly regulated/secure environments.

Features

- Business process analysis to optimise your processes
- Agile delivery methodology and project management expertise
- Custom applications development on the Servicenow platform
- Full ServiceNow managed services and support
- Hosting options: ServiceNow SaaS, customer private cloud, customer on-prem
- Experienced delivering ServiceNow into secure environments
- Full product lifecycle delivery
- Consistent customer outcome focus
- Test Automation using ServiceNow's Automated Test Framework (ATF)
- Developed Vetting (DV) and Security Check (SC) cleared staff

Benefits

- Optimised ServiceNow solution design to maximise output
- Clear and effective management of your delivery
- Delivery aligned to your organisational needs
- Secure and policy compliant platform that meets SLAs
- Hosted wherever is best for your business, including secure/regulated environments
- Delivery to meet all Government security requirements
- Reduced risk through end-to-end delivery services
- 360 engagement with your users to understand their requirements
- Collaboration to define your ServiceNow Strategy
- Accelerate your time-to-value realisation

Architecture and Design
Solution Delivery

An architecture and design service that translates business needs into secure, scalable cloud and digital solutions. It develops enterprise, technical, security and data architectures, simplifies complex problems and guides solution design across cloud environments. The service supports effective decision-making and enables successful modernisation and transformation outcomes.

Features

- Enterprise and technical architecture development
- Security architecture aligned to recognised frameworks
- Data architecture covering lifecycle, flows and integration
- Integrated architecture across systems and domains
- Cloud-ready designs enabling modernisation and transformation

Benefits

- Clear translation of needs into technical solutions
- Improved coherence across architectures and systems
- Reduced complexity and design-related risk
- Stronger foundations for digital transformation
- Secure, scalable architectures supporting future growth

Cloud Infrastructure and Apps
Solution Delivery

A cloud engineering service that designs and delivers secure, scalable infrastructure and application platforms across AWS, Azure, hybrid and cross-cloud environments. It transitions organisations from legacy systems or develops new bespoke solutions, ensuring compliant architectures, security controls and cloud-native practices that support resilient, efficient and future-ready operations.

Features
- Secure-by-design cloud architecture development
- AWS, Azure, hybrid and cross-cloud engineering
- Adoption of cloud-native services and patterns
- Security and compliance assessment against recognised frameworks
- Bespoke design supporting legacy transition and integration

Benefits
- Architectures tailored to client cloud strategies
- Improved security, resilience and scalability
- Reduced risk through structured cloud engineering
- Optimised cloud usage and operational efficiency
- Flexible, future-ready platform foundations

Cloud Migration
Solution Delivery

A cloud migration service that designs secure architectures, plans transitions and delivers automated deployments across public, private and hybrid environments. It assesses existing services, engineers cloud-ready solutions and manages migration activities for bespoke and COTS systems. The service enables assured, scalable and compliant cloud adoption for critical operational capabilities

Features
- Migration planning and transition management
- Automated deployment pipelines and configuration
- Public, private and hybrid cloud support
- Azure, AWS and customer-hosted environments
- Delivered in compliance with assurance requirements for Secure-by-Design
- Compliance, governance and risk alignment
- Cloud optimisation and configuration assessment
- Engineering for bespoke and COTS solutions

Benefits
- Tailored migration aligned to client environments
- Reduced complexity in secure cloud transitions
- Technology-agnostic assessment of cloud options
- Improved compliance and governance assurance
- Enhanced operational resilience and scalability

Secure AI Implementation
Solution Delivery

A service for secure AI consultancy to help organisations adopt, deploy and govern AI safely in secure and regulated environments. We design and implement AI solutions aligned to defence and government assurance requirements, supporting cloud, hybrid and air-gapped deployments while ensuring security, observability and responsible use throughout the AI lifecycle.

Features
- Secure-by-design AI architectures
- Cloud, hybrid and air-gapped deployments
- AI governance, risk assessment and guardrail design
- Protection of sensitive data and model sovereignty
- Integration with existing systems and workflows
- AI observability, monitoring and auditability
- Responsible-AI policies and control mechanisms
- Training and hands-on enablement for teams

Benefits
- Confident adoption of AI without compromising assurance
- Reduced risk from uncontrolled or opaque AI use
- Solutions aligned to data sensitivity and secure environments
- Strong governance and accountable AI operations
- Improved efficiency without increased security exposure
- Trusted, explainable outputs that support decisions
- Sustainable, assured AI capability within the organisation

Secure Collaborative Working Environments (CWE)
Solution Delivery

A service that designs and delivers secure collaborative working environments enabling organisations to communicate and share information with partners at required classification levels. It develops secure-by-design architectures aligned to government security standards such as CSMv4, producing controlled, compliant platforms for assured collaboration across cloud, hybrid and air-gapped environments.

Features
- Secure-by-design delivered solutions aligned to standards like CSMv4
- Design and delivery of partner-ready collaboration environments
- Cloud, hybrid and air-gapped deployment options
- Information controls supporting multi-organisation workflows
- Full engineering and transition into live service

Benefits
- Assured collaboration with partners at required classification levels
- Environments built to recognised secure-by-design standards
- Reduced risk through controlled, compliant platform architecture
- Tailored solutions comparable to DISX where required
- Reliable, scalable platforms supporting mission-critical collaboration

Public Cloud Secure Configuration

Solution Delivery

Specialists in configuring environments and applications hosted in public cloud to meet Government mandated security and operational requirements. We help plan public cloud deployments, re-engineer existing solutions and can apply security and functional improvements to gain maximum benefit from cloud. Specialists in AWS, Azure, hybrid and cross-cloud architectural solutions.

Features

- Secure configuration of AWS, Azure, Google and hybrid environments
- Adoption of cloud-native security controls and patterns
- Compliance alignment to NCSC and HMG security frameworks
- Security reviews across cloud and infrastructure components
- Configuration improvements for performance and resilience
- Security audit of existing cloud environments

Benefits

- Secure, compliant public cloud environments
- Reduced risk through improved configuration assurance
- Optimised cloud performance and cost efficiency
- Better alignment with organisational and government standards
- Stronger foundation for transformation and cloud adoption

Security Cleared Support Desk

A support desk service operated by security-cleared staff, providing incident management, service requests and user support aligned to ISO/IEC 20000 practices. The service is delivered through our accredited service management platform and configured to customer requirements, enabling reliable, controlled and auditable support operations in secure environments.

Features

- Security-cleared service desk personnel
- ISO/IEC 20000-aligned service management
- Customer-specific support workflows
- Incident and request management
- Asset and configuration tracking
- Secure communications and logging
- Integration with existing processes
- Performance and availability reporting

Benefits

- Assured support in secure environments
- Consistent, auditable service operations
- Reduced administrative and operational burden
- Faster issue resolution and response
- Alignment with established service standards
- Improved service visibility and reporting

LOGIQ

www.logiq.co.uk

We are ready to support your requirements.
Please contact us for further information:

contact@logiq.co.uk

Assured Service Provider
in association with National Cyber Security Centre
Consultancy: Risk Management

Assured Service Provider
in association with National Cyber Security Centre
Consultancy: Security Architecture

Assured Service Provider
in association with National Cyber Security Centre
Consultancy: Audit & Review