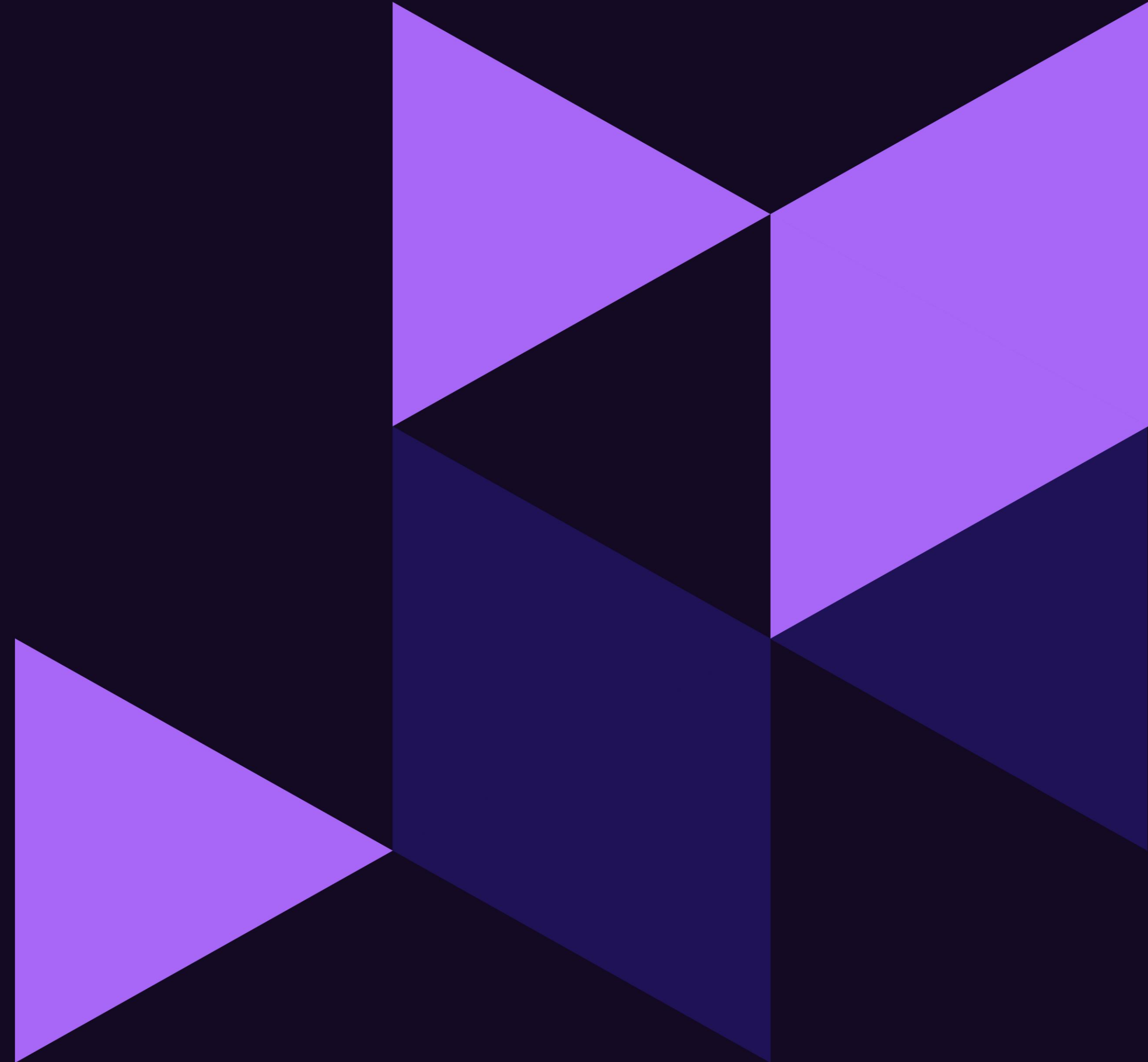


LAYER7

Cyber Security Architecture,
Risk & Compliance Services

G-Cloud Service Definition



Contents

About Layer 7

Why Layer 7

Who we work with

Cyber Security Architecture, Risk & Compliance Service Definitions

About Layer 7

Established in 2010, Layer 7 helps private and public sector organisations deliver and secure technology at pace. Our services include cyber security managed services and digital service delivery, technology skills enablement, legacy application transformation, data science, artificial intelligence and machine learning.

Layer 7 is a trusted supplier to central government departments, with a demonstrable track record of rapidly integrating with existing teams and quickly adding value. We are experts in delivering secure digital services founded on saleable platforms and are leaders in delivering digital, cloud-based platforms utilising modern engineering and architecture practices. We are specialists in both agile, waterfall and blended project delivery.

We work collaboratively with our clients to ensure we create a business focused, user-centred, evidence based, end-to-end secure services that reduce cost and greatly improve user experiences.

We understand how to deliver successfully, using a business outcome-based approach to deliver rapid results. This ensures we deliver against the highest priorities, maximise value and minimise waste.

At Layer 7 we strive for continuous improvement, learning and mentoring are part of our key values, and we are committed to sharing new and improved ways of working with our clients.



Your Trusted Secure Digital Partner

- We provide Cyber, Digital, Technology, Data and AI services to UK Public and Private Sector.
- Experts in modern cyber tradecraft, software engineering practices and architecture.
- Helping our clients build secure digital services and enhance their technology capabilities.
- Championing flexible, fast paced delivery and quality.
- Layer 7 is UKAS accredited 27001, 14001 , 9001, and holds Cyber Essentials Plus as well as being a Cyber Essentials Plus certification body since the scheme launch in 2014.



Service Definitions

Cyber Security Architecture, Risk & Compliance Services

- Cyber Security & Architecture Design
- NCSC Secure by Design (SbD) & Zero Trust
- Cloud Security Design
- Governance Risk and Compliance (GRC)
- Data Protection Impact Assessment (DPIA)
- Supplier & Supply Chain Assurance
- Operational Security Management and Risk Management
- Cloud Security & Gap Analysis

Cyber Security & Architecture Design

We design secure, scalable cyber security architectures aligned to business, cloud and NCSC requirements. Our experts embed security by design across systems, networks and applications, reducing risk, improving resilience, and enabling safe digital transformation across public and private sector environments.

layer7.uk

Service Features

- Secure-by-design architecture aligned to business and NCSC requirements
- Cloud, hybrid and on-premise security architecture design expertise
- Alignment with NCSC, ISO 27001, NIST and CIS Controls
- Zero Trust and defence-in-depth architectural patterns
- Threat modelling and risk-driven design decisions
- Architecture reviews for new and legacy systems
- Integration with DevSecOps and agile delivery models
- Identity, network, data and application security design
- Technology-agnostic, vendor-neutral architectural guidance
- NCSC Secure by Design SbD

Service Benefits

- Embeds Secure by Design principles aligned to NCSC guidance
- Supports NCSC Cyber Assessment Framework CAF compliance and assurance
- Reduces cyber risk through threat-led, Secure by Design architecture
- Improves resilience against nation-state and advanced persistent threats
- Enables Secure by Design cloud adoption aligned to NCSC principles
- Strengthens public sector assurance through NCSC-aligned security design
- Aligns systems to NCSC Secure by Design principles
- Simplifies complex environments with clear security architecture
- Information Security risk assessment and assurance
- Alignment of cloud security strategy with core information security strategy

NCSC Secure by Design (SbD) & Zero Trust

We deliver Secure by Design (SbD) and Zero Trust services for HMG programmes and projects. We provide continuous cyber security assurance aligned with NCSC guidance, NCSC CAF, NIST CSF, NIST SP-800-53, ISO27001, GovAssure, Data Protection Act and GDPR requirements, ensuring robust protection throughout the system lifecycle.

layer7.uk

Service Features

- Risk Assessment, Treatment, Security Management Plans and Security Cases
- Legacy HMG accreditation to Secure by Design transition support
- IAO and SRO liaison for governance and accountability alignment
- NCSC CAF, NIST CSF, GovAssure audits and compliance reviews
- Continuous assurance delivering through-life security management
- Cyber security policy development, standards advice and reviews
- HMG SbD self-assessment question set completion support
- Vetted Practitioner, Senior and Lead security consultants
- Independent, transparent Assurance and Accreditor oversight provision
- Supply chain cyber security risk assessment and management

Service Benefits

- Integrated approach eliminating duplication, reducing bureaucracy and costs
- Security as business enabler, not a project blocker
- Effective cyber security embedded across digital services and infrastructure
- Risk management integrated into programme governance from inception
- Continuous risk management reducing cyber threats and breaches
- Agile, pragmatic and proportionate security solutions delivered faster
- Informed risk ownership enabling confident executive decision-making
- Streamlined IAO and SRO relationships accelerating sign-off processes
- Proven expertise across Official, Secret and Top Secret classifications
- Zero Trust architecture principles embedded throughout security design

Cloud Security Design

Our Cloud Security Design service defines and implements secure, compliant cloud architectures aligned to NCSC guidance, HMG policy and industry standards. We design proportionate controls, embed security into agile delivery, and enable continuous monitoring, resilience and data protection across single and multi-cloud environments.

layer7.uk

Service Features

- Risk Assessment, Treatment, Security Management Plans and Security Cases
- Legacy HMG accreditation to Secure by Design transition support
- IAO and SRO liaison for governance and accountability alignment
- NCSC CAF, NIST CSF, GovAssure audits and compliance reviews
- Continuous assurance delivering through-life security management
- Cyber security policy development, standards advice and reviews
- HMG SbD self-assessment question set completion support
- Vetted Practitioner, Senior and Lead security consultants
- Independent, transparent Assurance and Accreditor oversight provision
- Supply chain cyber security risk assessment and management

Service Benefits

- Reduces cloud security risk through secure-by-design architecture
- Accelerates compliance with NCSC and government standards
- Protects sensitive data across cloud services and platforms
- Embeds security seamlessly into agile delivery pipelines
- Improves resilience and threat detection capabilities
- Enables confident adoption of public cloud services
- Reduces operational overhead through security automation
- Strengthens governance and architectural assurance decisions
- Supports scalable, cost-effective and secure cloud solutions
- Delivers safer, faster digital service deployment

Governance, Risk & Compliance (GRC)

Risk Management, Information Assurance and Compliance to HMG. Security, information assurance strategy and policy development, risk assessment, risk management, technical security design, Security Policy Framework (SPF) , CAF, NIST and ISO27001 compliance support, audit and review.

Service Features

- Cyber security policy, cyber security standards and cyber security procedures
- Qualified Information Assurance and Risk Assessors CRISC, CISM, ISO27001, CCP
- Full Risk Management, Governance and Compliance lifecycle
- Risk Assessment, Technical, Procedural, Legal, Compliance & Personnel controls
- Risk Management Frameworks & Methodologies, Risk Appetite identification & definitions
- Risk treatment planning, Risk monitoring
- ISO27000 series, CAF, Security Policy Framework (SPF) compliance consultancy
- GRC Tooling, Information Assurance (IA) policies & procedures

Service Benefits

- Integration into Agile Development Teams
- Ensures information assurance (IA) is an enabler, not a constraint
- Increased awareness of IA controls, policies and procedures
- Identification, assessment and prioritisation of risks to information assets
- Deliver Risk Management methodologies across the enterprise
- Development of risk aware enterprise culture
- Proactive ongoing risk management

Data Protection Impact Assessment (DPIA)

We provide proportionate Data Protection Impact Assessments aligned to GDPR, the Data Protection Act 2018 and Information Commissioner's Office guidance. Our DPIAs evaluate necessity, proportionality and privacy risks, define mitigations, and support accountability obligations for lawful, transparent personal data processing.

layer7.uk

Service Features

- DPIAs aligned to GDPR, DPA 2018 and ICO guidance
- DPIA screening to confirm high-risk processing requirements
- Clear definition of processing scope, context and purpose
- Assessment of lawful basis, necessity and proportionality
- Identification and evaluation of privacy and data protection risks
- Practical, prioritised risk mitigation measures documented
- Covers surveillance, profiling and special category data processing
- Consultation with internal and external stakeholders where required
- DPIA templates, policies and repeatable processes provided
- Support implementing agreed privacy risk controls

Service Benefits

- Evidences compliance with UK data protection legislation
- Reduces regulatory, reputational and operational privacy risk
- Enables lawful and transparent use of personal data
- Strengthens accountability and audit readiness
- Improves senior visibility of privacy risks
- Identifies international transfer and third-party risks early
- Embeds privacy by design across services
- Develops internal capability through knowledge transfer
- Supports consistent and repeatable DPIA delivery
- Delivered flexibly on-site or remotely

Supplier & Supply Chain Assurance

We deliver independent supply chain assurance assessments to help organisations understand and manage third-party cyber and data protection risks. Aligned to ISO 27001, NCSC Cyber Assessment Framework, DPA and GDPR, our audits provide proportionate assurance of supplier security controls, contractual obligations and ongoing risk exposure.

layer7.uk

Service Features

- Bespoke supplier assurance assessments aligned to organisational risk appetite
- Pre-onboarding supplier security and due-diligence assessments
- Prioritised risk reporting highlighting key supplier weaknesses
- Ongoing supplier assurance throughout the contract lifecycle
- Assessments aligned to legislation, regulation and sector requirements
- Review of contracts for security and assurance obligations
- Support for suppliers to remediate identified security gaps
- Remote, onsite and self-assessment audit delivery options
- Physical security audits using CMAT and STaMP
- Use of ISO 27001, NCSC CAF and NIST frameworks

Service Benefits

- Improves visibility of third-party security risks
- Enables informed supplier risk ownership and decisions
- Provides assurance beyond basic compliance checklists
- Supports proportionate, risk-based supplier management
- Reduces cyber and data protection exposure
- Delivers independent, vendor-neutral assurance
- Strengthens governance of supplier relationships
- Supports public sector assurance and audit requirements
- Tailored assessments aligned to organisational needs
- Proven experience delivering supplier assurance successfully

Operational Security Management and Risk Management

We design and implement operational security management capabilities for government organisations, enabling effective risk management and secure cloud adoption. Using proven architectures and security patterns, we align operational security to business objectives, improving visibility, resilience and threat response across live services.

layer7.uk

Service Features

- Operational security strategy aligned to business and risk priorities
- Security operations design using proven architectures and patterns
- Cloud-focused operational security capability development
- Security governance support aligned to HMG Security Policy Framework
- Automation and integration of operational security controls
- Threat modelling and attack scenario analysis
- Cyber risk assessment for live services and platforms
- Security representation within programme and delivery governance
- Protective monitoring capability design and assurance
- Delivery management across operational security initiatives

Service Benefits

- Enables risk-driven, business-aligned operational security decisions
- Improves operational security posture and threat awareness
- Supports secure operation of cloud-based services
- Delivers user-focused and outcome-driven security operations
- Reduces security risk to live digital services
- Strengthens governance and operational accountability
- Applies recognised security standards and frameworks consistently
- Combines security expertise with organisational change capability
- Enhances resilience through proactive threat management
- Proven experience securing central and local government services

Cloud Security & Gap Analysis

We can drive positive security transformation for your business by designing or reviewing cloud service architecture. We ensure it meets your business needs and security requirements, mitigates security risks, and complies with relevant policies and regulations, all while balancing information and business risks against the cost of controls.

layer7.uk

Service Features

- Assessment of security posture before procuring cloud services
- Evaluation of supplier compliance with an information security framework
- Validation of cloud architecture for compliance with security frameworks/standards
- Verification of security practice implementation in alignment with frameworks/standards
- Assessment of maturity and future roadmap for cloud investments
- Review and conduct threat modelling to identify risks and controls
- Workshops to deep dive into cloud security patterns

Service Benefits

- Compliance with industry and government security standards and best practices e.g. CAF, NIST CSF
- Security architecture assessment and maturity review of cloud services
- Consistent processes across cloud providers and business units
- Integration of regulatory compliance into design and review
- Information security risk assessment and assurance
- Design and review of resilient cloud infrastructure
- Alignment of cloud security strategy with core information security strategy
- Defined cloud security patterns based on standards and best practices
- Established designs to accelerate the adoption of secure cloud architecture

LAYER 7

layer7.uk

info@layer7.uk

layer7.uk

