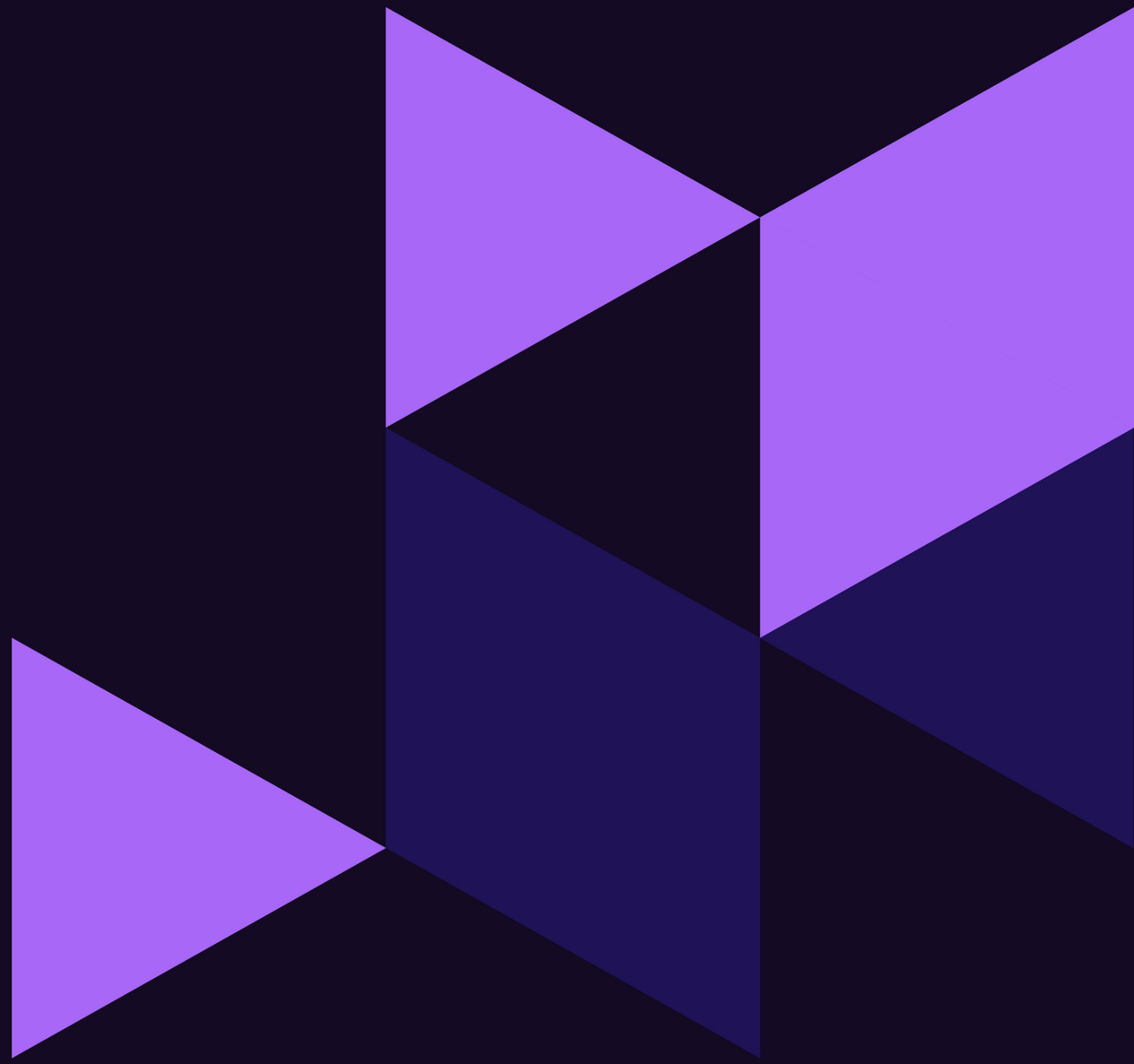
LAYER 7

Cyber Security Assurance, Testing & Operational Services

G-Cloud Service Definition



layer7.uk

Contents

About Layer 7

Established in 2010, Layer 7 helps private and public sector organisations deliver and secure technology at pace. Out 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 Assurance, Testing & Operational Services

- IT Health Check (ITHC)
- Red / Purple Teaming & Threat Led Penetration Testing
- Cloud, API, Mobile, OT/ICS Security Testing
- CVM & Continuous Security Controls Testing
- Incident Response Planning
- Cyber Essentials / Cyber Essentials+ (CE+)
- Security Awareness & Training
- Security Audit & review

IT Health Check (ITHC)

We deliver independent IT Health Checks using CHECK and CREST-aligned methodologies to identify security weaknesses across applications, infrastructure and cloud environments. Our accredited testers assess technical vulnerabilities, configuration weaknesses and control effectiveness, providing clear, risk-based findings to support remediation and assurance decisions.

layer7.uk

Service Features

- CREST and Cyber Scheme accredited security testers
- Testing aligned to OWASP, ASVS, MASVS, OSSTMM and PTES
- Application, infrastructure, cloud and mobile security testing
- Internal, external and remote-access security assessments
- Server, endpoint and network device configuration reviews
- Review of patching across operating systems and applications
- Assessment of authentication and authorisation controls
- Remote access and BYOD configuration reviews
- Identification of perimeter and internal security weaknesses
- Assessment of technical, procedural and physical security gaps

Service Benefits

- Provides clear, prioritised understanding of security risks
- Improves protection of business systems and information
- Delivered by experienced, independently accredited security specialists
- Produces clear reports with actionable remediation guidance
- Supports informed risk management and assurance decisions
- Identifies weaknesses before exploitation occurs
- Provides evidence for compliance and assurance requirements
- Cost-effective advice focused on practical remediation
- Proven experience delivering ITHCs across public sector organisations
- Builds confidence in the organisation's security posture

Red / Purple Teaming & Threat Led Penetration Testing

We deliver red and purple team exercises and threat-led penetration testing to simulate realistic adversary behaviour against live environments. Using intelligence-driven scenarios, we assess detection, response and resilience, providing evidence-based insight to prioritise remediation and strengthen long-term cyber defence strategies.

layer7.uk

Service Features

- Threat-led penetration testing based on realistic adversary scenarios
- Red team simulations across technical, physical and human attack vectors
- Purple teaming combining attack execution and defensive improvement
- Planned, sustained attack campaigns over extended assessment periods
- Exercises aligned to defined objectives and business impact
- Testing across internal, perimeter, cloud and hybrid environments
- Validation of detection, response and escalation capabilities
- Data exfiltration and impact demonstration where appropriate
- Structured planning, execution, reporting and lessons-learned cycles
- Actionable outputs prioritised by risk and exploitability

Service Benefits

- Tests security controls against realistic threat actor behaviours
- Provides deep insight into organisational cyber resilience
- Improves detection, response and recovery capabilities
- Aligns security investment to real-world threat priorities
- Strengthens collaboration between offensive and defensive teams
- Identifies gaps missed by traditional penetration testing
- Enables evidence-based security strategy and planning
- Supports prioritised, risk-driven remediation decisions
- Tailored exercises aligned to organisational risk appetite
- Increases confidence in security posture under real attack

Cloud, API, Mobile, OT/ICS Security Testing

We deliver specialist security testing across cloud platforms, APIs, mobile applications and OT/ICS environments. Using risk-based, standards-aligned methodologies, we identify vulnerabilities, misconfigurations and weaknesses, providing clear remediation guidance to improve resilience, protect critical services and support assurance requirements.

layer7.uk

Service Features

- Cloud security testing across AWS, Azure and GCP
- API security testing covering authentication, authorisation and data exposure
- Mobile application security testing for iOS and Android
- OT and ICS security assessments for operational environments
- Configuration and architecture reviews for cloud services
- Testing aligned to recognised industry and government standards
- Assessment of identity, access and secrets management
- Secure integration testing across hybrid and connected systems
- Risk-based reporting with prioritised remediation actions
- Flexible delivery including remote and on-site testing

Service Benefits

- Identifies vulnerabilities across modern and legacy environments
- Improves security of cloud-native and connected services
- Reduces risk of service disruption and compromise
- Protects sensitive data and critical operational systems
- Supports compliance and assurance evidence requirements
- Provides clear, actionable remediation guidance
- Strengthens resilience of APIs and digital integrations
- Improves confidence in mobile and cloud deployments
- Enables informed risk-based security decisions
- Enhances overall cyber security posture

CVM & Continuous Security Controls Testing

We deliver Continuous Vulnerability Management and security controls testing to provide ongoing assurance of cloud and enterprise environments. Using automated tooling, threat intelligence and adversary-led techniques, we identify weaknesses early, validate control effectiveness and support continuous risk reduction aligned to business priorities.

layer7.uk

Service Features

- Continuous vulnerability scanning across cloud and enterprise environments
- Automated controls testing integrated into live operational environments
- Cloud-native security visibility using Wiz platform
- Vulnerability identification and prioritisation using Tenable tooling
- Threat-led security controls testing aligned to realistic attack paths
- Validation of preventative, detective and corrective security controls
- Risk-based vulnerability prioritisation using exploitability and impact
- Continuous configuration and exposure management for cloud assets
- Actionable reporting mapped to remediation and risk ownership
- Delivered by experienced practitioners and Tenable Partner specialists

Service Benefits

- Provides continuous visibility of security weaknesses and exposures
- Prioritises remediation based on real-world threat likelihood
- Validates effectiveness of deployed security controls
- Reduces risk between periodic audits and assessments
- Improves cloud and enterprise security posture over time
- Supports evidence for assurance, audit and compliance activities
- Enables faster detection and response to emerging risks
- Reduces manual effort through automated security testing
- Aligns security investment to highest-risk attack paths
- Builds confidence in ongoing cyber resilience

Incident Response Planning

We work with executive leaders and technical teams to design, test and refine incident response plans tailored to your organisation. Our service ensures clear roles, effective decision-making and coordinated recovery, helping organisations respond confidently to cyber incidents while meeting regulatory and assurance requirements.

layer7.uk

Service Features

- Development and testing of incident response plans
- Crisis management planning and exercise support
- Tailored tabletop exercise scenario design
- Scenarios informed by real-world threats and intelligence
- Identification of lessons learned and improvement actions
- Clarification of roles and responsibilities during incidents
- Alignment with legislative and regulatory obligations
- Identification of gaps in processes and capabilities
- Executive and technical team engagement
- Repeatable incident response planning framework

Service Benefits

- Prepares organisations to respond effectively to cyber incidents
- Clarifies decision-making and accountability during incidents
- Supports compliance with legislative and regulatory requirements
- Aligns incident response to ISO 27001 controls
- Improves organisational resilience and readiness
- Provides structured, repeatable response processes
- Aligns with recognised incident response models
- Strengthens coordination between leadership and technical teams
- Reduces impact and recovery time following incidents
- Builds confidence in incident response capability

Cyber Essentials / Cyber Essentials+ (CE+)

We provide a managed Cyber Essentials Plus service, supporting organisations through assessment, remediation and certification. Our consultants guide you through the self-assessment, testing and verification process, delivering pragmatic advice and assurance to help you achieve CE+ efficiently and demonstrate protection against common cyber threats.

layer7.uk

Service Features

- Managed end-to-end Cyber Essentials Plus certification support
- Guidance completing and submitting the self-assessment questionnaire
- Fully managed external vulnerability scanning
- Internal user device assessments delivered remotely or onsite
- Pragmatic remediation advice to address identified gaps
- Optional pre-assessment to support first-time pass success
- Validation of scan results to remove false positives
- Re-testing included within defined remediation window
- Certification issued following successful assessment
- Delivered by experienced Cyber Essentials consultants

Service Benefits

- Simplifies achieving Cyber Essentials Plus certification
- Reduces risk of failure through expert guidance
- Ensures accurate vulnerability findings and validation
- Improves security of devices and organisational data
- Demonstrates cyber security maturity to customers
- Supports supplier assurance and supply-chain requirements
- Enables eligibility to work with government organisations
- Increases confidence when bidding for new business
- Inclusion on the National Cyber Security Centre certification directory
- Reassures stakeholders against common cyber threats

Security Awareness & Training

We deliver security awareness training that goes beyond compliance, using behavioural science to drive meaningful culture change. Our approach builds understanding, ownership and secure behaviours across organisations, helping teams actively support cyber resilience and contribute to shared security objectives.

layer7.uk

Service Features

- Security awareness programmes focused on behaviour & culture change
- Role-based cyber awareness training for diverse teams
- Upskilling programmes to strengthen organisational security capability
- Security organisational change management support
- Strategic cyber threat briefings for leadership teams
- Staff cyber awareness and practical security briefings
- Senior executive situational awareness sessions
- Gold team exercises for executive-level decision making
- Incident response awareness and consultation sessions
- Effective logging and security monitoring awareness briefings

Service Benefits

- Improves organisational security posture at low cost
- Encourages secure behaviours across the workforce
- Builds genuine engagement with security objectives
- Uses real-world scenarios and case studies
- Delivered by experienced cyber security practitioners
- Tailored to organisational risks and priorities
- Strengthens leadership understanding of cyber threats
- Reduces likelihood of human-driven security incidents
- Supports a cyber-resilient organisational culture
- Complements technical security controls effectively

Security Audit & Review

We deliver independent security audits and reviews to assess organisational resilience to cyber threats. Our consultants evaluate policies, controls and technical environments against recognised standards and regulatory requirements, providing objective insight, clear recommendations and practical improvement plans to strengthen security posture and governance.

layer7.uk

Service Features

- Review of security policies, standards and procedures
- Security audits aligned to recognised frameworks and methodologies
- Assessment of compliance against industry and regulatory requirements
- Evaluation of existing risk and assurance arrangements
- Audit planning aligned to organisational risk appetite and objectives
- Identification of control gaps and weaknesses
- Assessment of people, process and technology controls
- Recommendations supporting continuous compliance and improvement
- Independent, objective audit reporting and assurance
- Practical remediation planning and prioritisation support
- t

Service Benefits

- Provides independent assurance of security posture
- Strengthens internal controls and governance arrangements
- Supports compliance with statutory and regulatory requirements
- Identifies operational inefficiencies and control weaknesses
- Promotes adoption of security best practices
- Improves planning, prioritisation and investment decisions
- Enables informed, risk-based decision-making
- Enhances credibility with stakeholders and auditors
- Assesses effective and responsible use of resources
- Supports continuous improvement of security maturity

LAYER 7

layer7.uk

info@layer7.uk