G-CLOUD 15 SERVICE DEFINITION

Security Assurance

Transforming IT QA Services

Delivering secure, innovative and effective IT QA solutions tailored for client needs.

- ISO 27001 Certified
- Cyber Essentials Plus
- ISO 9001 Certified
- ISO 14001 Certified
- 88% KT retention
- 98% Client Satisfaction

Independent Security Assurance for Informed Decisions

Decision-Ready

Provides independent evidence to support business acceptance, release and go-live decisions for cloud-hosted digital services.

- Governance-ready outputs
- Evidence-based evaluation

Risk-Based Assessment

Assesses security readiness in the context of service risk, threat exposure and operational impact.

- Residual risk articulation
- Risk visibility & clarity

Assurance, Not Ownership

Operates as a decision-support control, not delivery or operational ownership. Provides objective validation without conflict of interest.

Clear Evidence Boundaries

Enables buyers to understand what has been evidenced, what remains untested and residual risks at decision points.

When Buyers Need This Service

Pre-Deployment Assurance

Prior to business acceptance or live deployment of new or materially changed digital services.

Sensitive Data Protection

Where services process sensitive, personal or business-critical data requiring independent security validation.

Separation of Duties

Where security risk must be assessed independently of delivery teams to maintain separation of duties.

Multi-Supplier Environments

Where multiple suppliers contribute and a neutral assurance position is required.

Governance Support

To support governance, audit or senior decision forums with objective, decision-ready security evidence.

Point-in-Time Assurance

Designed for stage-gated assurance aligned to formal decision points, not continuous security management.

This service is specifically designed to provide independent validation at critical decision junctures.

Service Scope and Boundaries

In Scope

- Independent assessment of security posture aligned to service risk and decision context
- Security testing scoped to agreed components, interfaces and deployment context
- Assessment of identity, access control, data protection and configuration practices
- Evaluation of security-related operational readiness affecting live-service risk
- Production of structured, decision-ready security assurance evidence for governance and audit
- Risk identification, classification and communication to influence acceptance decisions

Out of Scope

- Remediation or vulnerability fixing
- Managed, continuous or operational security services
- Live operational security ownership or monitoring
- Security certification, accreditation or compliance sign-off (Unless explicitly agreed)

Service Inclusions & Exclusions

Included

- ✓ Risk-based security testing focused on decision-critical exposure
- ✓ Evidence-based evaluation of security readiness for acceptance and go-live
- ✓ Clear articulation of security risks, limitations and residual exposure
- ✓ Structured assurance outputs suitable for governance and senior stakeholders
- ✓ Retest and revalidation assurance to confirm remediation effectiveness

Not Included

- ✗ Remediation, vulnerability fixing or implementation support
- ✗ Continuous testing, monitoring or SOC services
- ✗ Incident response, threat hunting or forensic investigation
- ✗ Live service security management or guarantees
- ✗ Compliance or certification ownership

Outputs are designed to be decision-ready, requiring minimal interpretation. Service provides assurance evidence, not delivery accountability.

Security Assurance Coverage & Techniques

- ✓ Risk-based security testing
- ✓ Access control assessment
- ✓ Independent review
- ✓ Coverage & confidence-based assurance

App Vulnerabilities

Assessment of business-critical functionality exposure.

API & Backend Security

Controls relevant to data protection and service integrity.

Auth & Authorisation

Session management and access control validation.

Configuration Security

Infrastructure posture impacting live-service risk.

OWASP Risk Classification

Identification aligned to decision-making needs.

Threat Scenarios

Attack-path analysis for decision-critical exposure.

⚠ Assessment limited to generating decision-ready assurance evidence only. Does not imply remediation responsibility.

Testing Limitations, Safeguards & Outputs

Testing Limitations & Safeguards

- Testing limited to agreed scope and authorised targets to protect service stability
- Techniques causing service disruption excluded unless explicitly agreed
- Production environments approached cautiously, aligned to buyer risk tolerance
- Assurance outcomes reflect observed evidence within scope, not exhaustive validation

Typical Assurance Outputs

- Security readiness and confidence statements
- Risk-classified findings mapped to decision impact
- Coverage and limitation statements clarifying what has and has not been evidenced
- Residual risk assessments to support acceptance or conditional acceptance
- Evidence packs suitable for governance and audit review

Decision-Focused Approach

Outputs are framed to answer decision questions. All evidence is designed to support informed business acceptance and go-live decisions.

Training & Knowledge Transfer: Enablement limited to helping Buyer representatives interpret assurance outputs.

Marketplace Positioning: Provides independent security assurance without transferring delivery risk or ownership.

Governance, Authority & Buyer Responsibilities

Testing Authority

All security activity conducted with explicit buyer authorisation and agreed scope.

Operates within legal, contractual and governance constraints defined by buyer representatives.

Does not replace buyer governance, security ownership or statutory accountability.

Buyer Responsibilities

Acceptance & Release Decisions: Buyer retains full decision-making authority.

Representatives: Nomination of appropriate decision makers.

Risk Ownership: Business and security risk remains with buyer ownership or management.

Formal Sign-Off: Required at agreed decision points.

Escalation

Material security risks classified by severity and decision impact.

Residual risk articulated clearly to support acceptance decisions.

Escalation limited to decision support, not issue ownership.

Service Entry & Exit

Entry: Service may be engaged at any stage where security assurance is required.
Exit: Service concludes on delivery of agreed assurance outputs.

Service Integration

This service may be used alongside Managed Testing Services where end-to-end ownership is required.

About Spectrum IT Hub Ltd

Spectrum IT Hub is a UK-based professional IT services provider delivering independent, evidence-based quality assurance and testing services. We support the delivery of accessible, usable and compliant digital services through a flexible onshore and offshore delivery model, aligned to UK public sector standards and assurance expectations.

Mission

To provide secure, high-quality and independent assurance services that support public sector organisations in making informed acceptance, release and go-live decisions for cloud-hosted digital services, through structured testing, governance and evidence-led assurance.

COMPANY DETAILS

COMPANY NUMBER

13649954

HEAD OFFICE

3 Newbridge Square, Swindon, England, SN1 1HN

OFFSHORE ADDRESS

No.6, 2nd floor, Jayanagar housing society layout, Uttarahalli Main Rd, 2nd Stage, Chikkalasandra, Bengaluru, Karnataka 560061

Delivery Model & Compliance Standards

Hybrid Delivery Model

Onshore

UK-based senior consultants and delivery managers providing stakeholder engagement, governance, assurance leadership and buyer-facing activities.

Offshore

Specialist global delivery teams providing cost-effective execution of testing activities under defined quality controls and governance.

Flexible Mix

Tailored to security constraints and buyer preferences.

Certifications & Standards

ISO Certified
27001 / 9001 / 14001

Cyber Essentials Plus
Government Accredited

GDS Service Standard
Alignment

WCAG 2.2 AAA
Accessibility Compliance

Proven Value & Track Record

100%

20-Day SLA Met

Consistent adherence to agreed mobilisation and readiness timelines

88%

People & Knowledge Retention

Through stable team continuity, structured KT, documentation and controlled handover

24/7

Support Coverage

Continuous support availability

99.5%

Defect-Free Delivery

With comprehensive test coverage and risk-based testing

98%

Client Satisfaction

Proven excellence with measurable outcomes

80%+

Repeat Engagements

Demonstrating trust, continuity and long-term partnerships

How to Engage (G-Cloud 15)

G-Cloud Marketplace Process

1 **Search the Marketplace**

Locate the Spectrum IT Hub – Security Assurance Services offerings.

2 **Statement of Work**

Define scope, objectives, environments and delivery timelines.

3 **Contract & Delivery**

Commence service delivery under agreed terms.

Support & Hours

Standard Working Hours

Monday to Friday: 09:00–17:00 (UK time)
Excluding UK public holidays.

Support Availability

- Email, ticketing and web chat support available during standard working hours
- High-priority issues impacting active testing acknowledged within accelerated timeframes
- Out-of-hours and weekend support available where agreed

Service Levels

Spectrum IT Hub provides tiered support aligned to cloud assurance and testing services:

- **Standard Support**
  Included during published support hours
- **Enhanced Support**
  Extended hours or faster response times during critical phases
- **Premium Support**
  24/7 availability or senior escalation where contractually agreed

Note: Support levels, availability and response targets are agreed in advance.

Contact Information

PRIMARY CONTACT

Arif Shaik

Programme QA Delivery Manager

arif.shaik@spectrumithub.com
+44 7468 341880

BACKUP CONTACT

Ranjith K

Senior Account Manager

ranjith.kanhirathingal@spectrumithub.com
+44 7539 568242

Our Other Quality Assurance & Testing Services

Assurance and Functional Testing

For building confidence that core functionality behaves as expected and supports informed acceptance decisions.

Automation Testing

For reducing manual testing effort and increasing consistency through reliable, repeatable automated coverage.

Accessibility & Usability Testing

For improving how real users experience your service, supporting inclusive, intuitive and accessible design outcomes.

Performance Testing

For gaining confidence that services can handle expected demand, load and operational pressures.

User Acceptance Testing (UAT)

For supporting confident business sign-off by validating readiness against agreed acceptance expectations.

QA Governance

For establishing control, visibility and consistency across testing activities and multiple suppliers.

End-to-End (E2E) Testing

For confirming that complete business journeys work seamlessly across integrated systems.

Managed Testing Services

For maintaining ongoing testing support under clear governance while delivery teams stay focused on outcomes.