G-Cloud 15 Service Definition Document

Application Security Testing and Code Review

Lot: Lot 3: Cloud Support Service

Affinity Digital (Technology) Limited

CONFIDENTIAL

Summary of Service

Structured application security testing and manual code review to identify vulnerabilities before they reach production. Affinity's security-first engineering team combines automated scanning with expert manual review, drawing on our own DevSecOps toolchain (Trivy, Semgrep, Gitleaks, TruffleHog, OWASP ZAP) and experience supporting clients through ITHCs and formal penetration tests. Suited to organisations needing assurance ahead of a security review, or wanting security embedded into an existing development pipeline.

Key Features

- Manual code review by experienced engineers, not automation alone
- Automated static analysis, secrets scanning, and dependency checking
- OWASP Top 10 and OWASP ASVS-aligned assessment
- Findings report with severity ratings and remediation guidance
- Optional integration of security tooling into client CI/CD pipelines
- Support through remediation and re-test

Key Benefits

- Identifies vulnerabilities before they reach production or a formal ITHC
- Reduces cost and disruption of late-stage security findings
- Combines automated coverage with human judgement automation alone misses
- Delivered by the same team that builds and supports live government services
- Can be a one-off assessment or an ongoing embedded practice

Service Standards

Affinity delivers services in line with the Technology Code of Practice, ensuring the relevant points of the TCoP are adhered to throughout delivery.

Security Standards: Affinity operates a security-first philosophy, with a dedicated Data Protection Officer and Senior Information Risk Owner, and a wealth of knowledge and experience delivering services which store data up to OFFICIAL-SENSITIVE classification.

Affinity holds Cyber Essentials Plus, which exceeds the standard Cyber Essentials baseline mandatory for all G-Cloud 15 suppliers on this lot.

- ISO 27001:2022
- ISO 9001:2015
- Cyber Essentials Plus (IASME)

Insurance and Financial Standing

Affinity holds combined professional indemnity, public liability, and employers' liability insurance meeting or exceeding the £7m minimum required under G-Cloud 15's Joint Schedule 3 for this lot.

Governance and Service Assessments

Our team has worked on a variety of projects required to follow the GDS Service Manual and meet the Service Standard. We work with the product owner to ensure that, where required, assessments are carried out throughout the project to support smooth service go-lives. Our dedicated team members assist stakeholders with service set-up and transitions through the entire lifecycle of digital services.

In any service assessment, our agile, collaborative approach and consistently user-centred stance, in line with the Service Manual and Service Standard, make it straightforward for the service owner to talk the panel through the service with confidence that it meets user needs and applicable standards.

To stay current we maintain subscriptions and monitoring across GOV.UK frontend toolkit repositories, Service Design Manual change notifications, relevant community channels, and a multi-disciplinary team who track the latest updates and releases.

Team Certifications

Delivery is supported by team members holding, or actively pursuing, recognised certifications including ISO 27001 Lead Auditor, CISM, and cloud-provider certifications (AWS, Azure). Named CVs are provided at proposal stage where a specific engagement requires them; this section describes the general capability pool rather than committing named individuals to every call-off.

Knowledge Transfer and IP Ownership

All custom deliverables produced for a client under this service become the client's property on completion, unless otherwise agreed in the call-off contract. Knowledge transfer is built into delivery rather than treated as a separate exit activity — documentation, runbooks, and architecture decision records are maintained throughout, not backfilled at offboarding.

External Testing

Penetration Tests

We regularly support clients through penetration tests and remediation of any resulting findings. This includes working with testers to provide appropriate access, confirming scope, ensuring tests do not adversely affect live service performance, resolving flagged issues, and revoking all temporary access on conclusion of testing.

We have worked with established CHECK/CREST-accredited testing providers on penetration tests for numerous public sector clients.

Security Reviews

Having worked through ITHCs and security assessments for government projects, our team implements security from the outset, minimising the need for remedial action ahead of formal reviews.

Accessibility Assessments

We have extensive experience supporting clients through accessibility assessments and remediation, working to WCAG 2.2 Level AA and the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018. We make use of automated tools (axe, WAVE, Lighthouse) alongside expert manual auditing, and have engaged external disability user-testing groups during iterative development to confirm services are fit for purpose.

Tiers of Support

P1 — Critical	Within 1 hour: identify & fix, or provide time-to-fix estimate
P2 — High	Within 1 working day: identify problem & provide time-to-fix
P3 / P4 — Standard	Within 5 working days: work commences within normal hours

Flexible Resource Model

Affinity is a full-service digital agency offering a full lifecycle service, on a blended day-rate model — meaning clients can engage the whole team (UX, design, solution architecture,

service design, development, security) rather than only named specialists, without rate variation by role.

We understand support and continual improvement work has natural peaks and troughs, and we manage this with a dedicated Technical Lead and Account Manager, supported by developers who build interchangeable depth of knowledge of each client's environment so the team can flex as needed.

Availability and Response Times

We track resource usage against activity using Jira and Harvest, and can offer 24/7/365 support for critical environments, drawing on our own team and established infrastructure partners. Response targets by priority are summarised below.

- Priority 1 (P1) — very urgent bugs seriously impacting a range of services or operations: Affinity will, within 1 hour of an agreed P1, endeavour to identify and fix the problem or provide a time-to-fix estimate, prioritising all available resources as needed.
- Priority 2 (P2) — bugs seriously impacting a narrower range of operations: Affinity will, within 1 working day, endeavour to identify the problem and provide a time-to-fix; work paused to prioritise P1s resumes at the earliest opportunity.
- Priority 3 (P3) and Priority 4 (P4) — other bugs: Affinity will endeavour to commence work within 5 working days of acknowledged receipt, within normal working hours.

Communication on Support

Affinity uses Jira Service Management to handle support and maintenance, with service users able to raise requests via a dedicated Service Desk portal or a monitored support mailbox that automatically raises a ticket.

As part of onboarding, workflows, notification schemes, response times and other service parameters are configured according to agreed service levels. We use Jira work-logs, integrated with Harvest, to estimate, record, and track time spent on each ticket, giving clients a clear, reportable view of support activity.

We agree on the nature and frequency of account-level reporting at the start of engagement — typically including service usage, KPIs (time to resolution, availability/up-time, service breaches), and timesheet reporting. Monthly service review meetings with the account manager provide a regular opportunity to review delivery and identify improvements.

Affinity Project Management

Affinity recognises there is no single methodology that fits every client, and offers Agile, Waterfall, and a Hybrid Agile approach, tailored early in engagement to match a client's own process maturity. The diagram below shows the general shape of engagement from initial discovery through to offboarding, common across all our services.

Agile

Our full Agile process uses an iterative backlog definition and refinement cycle feeding a core development scrum, following industry-standard practice and compatible with larger-scale frameworks such as SAFe. This is a highly collaborative approach with regular stand-ups, refinement sessions, and story-card workshops.

Waterfall

For clients seeking a traditional engagement, we work through a formal elaboration phase to detail requirements, then deliver against an agreed budget and specification, dividing the requirement internally and iteratively developing it within our core team to manage change control.

Hybrid Agile

Where full cross-organisational Agile isn't yet achievable, our Hybrid approach proposes proven open-source packages, modules, and templates offering the solution largely 'out of the box', paired with a lightweight Agile backlog — reducing the detailed requirements work of a full Agile engagement while retaining an auditable, recognisable Agile structure with fortnightly show-and-tells and phased or single-point releases.

Onboarding

When onboarding services from an incumbent supplier, Affinity follows a structured process: agreeing roles and responsibilities across both organisations, agreeing timescales for a progressive or single-point handover, tracking all onboarding actions to completion, and securing all relevant access (SSO/identity systems, cloud accounts, code repositories, server access, collaboration tools, and the incumbent's issue tracker).

We seek access to all relevant documentation and code — version-controlled codebases, architecture and application documentation, disaster recovery procedures, BAU documentation, runbooks, prior penetration test/accessibility/load test/DR rehearsal outcomes, and the existing support knowledge base and ticket history.

Where possible we validate processes and access alongside the outgoing supplier before go-live, surfacing and resolving practical issues (build/deployment quirks, missing access rights) ahead of time to ensure the smoothest possible handover, and ensuring open support tickets are transferred appropriately for continuity of service.

Exit Plan & Data Portability

Every engagement includes an agreed exit plan covering how client data will be extracted in a usable, non-proprietary format, how transition to a new supplier (or in-house team) will be

managed, and what assistance Affinity provides during handover. This is established during Elaboration, not improvised at contract end.

Data extraction timescales and formats are confirmed per service; as a baseline, Affinity commits to providing a full data export and current documentation set within the offboarding notice period below.

Supply Chain & Sub-processors

Affinity does not employ any offshore staff or sub-contractors, and does not use offshore delivery services. Our delivery model scales using trusted UK-based colleagues who work to Affinity's own ways of working, QMS processes, and security requirements.

Data Residency

Client data is hosted in UK regions of our cloud infrastructure partners (AWS, Azure) by default. Any exception requires explicit client agreement and is documented as part of service onboarding.

Offboarding

Affinity actively seeks long-term relationships and, as a full-service digital agency, offers a full lifecycle service — but takes offboarding as seriously as onboarding. We work with clients during elaboration to establish an offboarding strategy based on our tried-and-tested model, flexed to the client's needs, including the ability to offboard for any reason with a minimum of 3 months' notice.

Disaster Recovery

Affinity works collaboratively with clients to minimise risk, establishing appropriate Disaster Recovery plans so that, in the event of a crisis, a well-planned and thoroughly tested recovery process is in place. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are established with clients to inform backup policy, with the DR plan tested against measurable, verifiable criteria.

Responsibility for Business Continuity and Disaster Recovery (BC/DR) is allocated according to the roles and responsibilities of our ISO 27001:2022-based Information Security Management System, and BC/DR arrangements are tested at least annually.