

G-Cloud 15

Service Definition

Zoonou Limited

Web Application Penetration Testing

Lot 3: Cloud Support

January 2026



National Cyber
Security Centre



01. About Zoonou	4
Who we are	4
What we do	4
How we work	4

02. Our experience	5
Central Government and Arm's-Length Bodies	5
Housing and Citizen Services	5
Health and Regulated Digital Services	5
Charities and Not-for-Profit Organisations	6
Higher Education	6
Museums, Heritage and the Arts	6

03. Overview of the G-Cloud Service	6
Penetration Testing Scope	7
Methodology, Process and Reporting	7
Governance and Reporting	7
Vulnerability Assessments	7
Other Cyber Security Services	8

04. Assurance and security	8
We're a CREST member company	8
ISO 27001 - Information Security	8
ISO 9001 - Quality Management	8
ISO 14001 - Environmental Management	8
Cyber Essentials and Cyber Essentials Plus	8
Gold Partner - International Software Testing Qualifications Board (ISTQB)	8
BPSS (Baseline Personnel Security Standard)	8

05. Delivery models	9
Embedded QA	9
Outsourced QA	9
Dedicated QA Team	9
Project-based QA	9
Location and integration	9

06. Using the service	9
------------------------------	----------

Pricing	9
Availability of trial service	9
Ordering and invoicing	9
Onboarding	10
Implementation and delivery approach	10
Training	10
Technical requirements and client-side requirements	10
After-sales support	10
Offboarding	10
Termination process	10
Service constraints	10
Backup and restore details	10
Service levels	10
Data restoration and service migration	10
07. Social value	11
Tackling economic inequality	11
Fighting climate change	11
Increasing supply chain resilience	11
Building healthier communities	11
Driving innovation	11
08. Other QA services	12
09. Contact details	12
Rhodri Alexander	12

01. About Zoonou

Zoonou is a UK-based digital quality assurance company. We're a small-to-medium enterprise (SME), with a full-time team and a history of organic growth - no external investors, allowing us to stay focused on quality, long-term partnerships and responsible delivery.

Who we are

We're the UK's only [employee-owned software testing company](#) and [a certified B Corp](#). Founded in 2007, we specialise in quality assurance (QA) and software testing, helping public and third sector organisations - and their delivery partners - create digital services that people can rely on.

We work with teams delivering citizen-facing and business-critical services, where quality, accessibility and trust really matter. Our role is to provide independent assurance and practical support - helping teams reduce risk, meet standards and feel confident about releasing and running digital services.

Because we're employee-owned, everyone at Zoonou has a real stake in the quality of our work and the relationships we build. As a B Corp, we balance commercial success with positive outcomes for users, clients, and society.

What we do

We support quality across the entire delivery lifecycle - from early planning and strategy to hands-on testing and ongoing assurance for both new and live digital public services.

Our multidisciplinary teams provide:

- Risk-based QA strategy aligned to service goals and governance needs.
- Evidence-based insights to support go-live decisions, governance and audits.
- Ongoing QA support to help protect service quality as systems change and grow.

We work closely with teams to share knowledge, strengthen processes, and build internal QA capability, ensuring teams are stronger and more confident long after engagement.

How we work

Every organisation works differently - especially in the public sector, where teams balance pace, accountability, transparency, and high expectations from users and stakeholders. We focus on building strong, trusted working relationships that support confident decision-making and sustainable delivery.

We look to add value early and often, working with teams from the outset to understand service goals, risks, governance needs, and constraints. This allows us to provide proportionate, risk-based assurance and help teams adopt best practices that fit their context, rather than imposing a one-size-fits-all approach.

We work in close partnership with in-house teams, delivery partners, and other suppliers, recognising that public services are often delivered through multi-supplier environments. Our approach is collaborative and evidence-led, with clear communication and practical recommendations designed to support decisions at all levels - from delivery teams through to senior stakeholders and assurance boards.

For more details on what you can expect from us - and what we promise to bring to every partnership, [read our client charter](#).

02. Our experience

We work with organisations delivering citizen-facing and business-critical services across the public and third sectors. We bring practical sector expertise to every engagement, helping teams meet statutory standards, pass assurance and assessment processes, and deliver services that are reliable, inclusive, and ready for live use.

Central Government and Arm's-Length Bodies

We support central government departments, executive agencies, and arm's-length bodies to improve service reliability, reduce operational risk, and provide confidence in complex digital programmes.

Case study: Natural Resources Wales (NRW)

Since 2019, we've supported NRW to [strengthen the resilience, security, and reliability of their mission-critical digital systems](#). Our work includes penetration and load testing as well as accessibility audits of public-facing services like flood warning and telemetry platforms. This helped NRW improve operational resilience, protect communities with timely alerts, and support data-driven decision-making.

“Zoonou’s support has been key in helping NRW strengthen the resilience and accessibility of our systems, so we can better protect communities and the environment.” - Dean Johnson, Test Manager.

Housing and Citizen Services

We work with housing associations and public service providers to make it easier for residents to access services and get the support they need efficiently.

Case study: Southern Housing Group (SHG)

We supported [multiple digital transformation programmes, focusing on data migration, integration testing, and risk-based QA](#). By identifying potential issues early and validating data flows, we reduced delivery risk, ensured continuity of critical services, and improved confidence in new digital platforms.

“Zoonou are quick to understand requirements, take the time to listen, sometimes at very short notice, and have always delivered to align Zoonou’s services to my team’s requirements, equally impressing the Programme and Project Managers.” - Will Brimble, Implementation Manager.

Health and Regulated Digital Services

We support health and social care organisations, including NHS bodies and central government health departments, to deliver better healthcare outcomes while meeting stringent regulatory and safety requirements.

Case study: Department of Health and Social Care (DHSC)

Under a G-Cloud framework, we've supported multiple DHSC workstreams, including the NHS Couch to 5K app, combining functional testing, haptics validation, and penetration testing. Our structured QA identified risks early, ensured robust performance, and provided evidence for assurance and future development planning.

**“Great team, always professional, responsive and flexible to support our requirements.” - Jimmy
Carnie, Digital Product Lead.**

Charities and Not-for-Profit Organisations

We work with charities and not-for-profit organisations to increase reach, improve service delivery, and demonstrate impact to stakeholders.

Case study: The King’s Trust (formally The Prince’s Trust)

We delivered [performance and functional assurance for a fundraising and step-tracking app, covering load testing and risk-based QA](#). Our testing ensured the app could handle real-world usage, maintain data integrity, and provide a reliable experience, enabling the charity to launch on time and demonstrate system resilience.

“Zoonou were flexible and adaptable on a project with numerous stakeholders and delivered a test approach that accommodated a lot of moving parts.” - Tom Fernandes, Project Manager.

Higher Education

We work with higher education institutions to enhance learning, streamline operations, and strengthen institutional reputation globally.

Case study: Imperial College London

We help embed accessibility across Imperial’s digital services, from staff training and audits to ongoing advisory support and internal presentations. This strengthens digital governance, improves accessibility for students and staff, and ensures platforms meet regulatory and institutional standards.

Museums, Heritage and the Arts

We support cultural and heritage organisations to deliver engaging digital experiences that inspire audiences and extend reach beyond physical sites.

Case study: British Film Institute (BFI)

Since 2020, we’ve helped the BFI [embed accessibility across their organisation](#). Our work includes training, strategic guidance, regular audits, proactive design reviews, and testing with users with disabilities. This has improved audience experiences, ensured compliance with public sector accessibility standards, and embedded accessibility from design through delivery.

03. Overview of the G-Cloud Service

Our Web Application Penetration Testing services help public sector organisations protect citizen-facing and internal web applications.

We identify security risks, vulnerabilities, and misconfigurations, supporting compliance with GDS Service Standards, UK GDPR, [Secure by Design Principles](#), and the [National Cyber Security Centre \(NCSC\) guidance](#), including preparation for IT Health Checks (ITHC), accreditation, and ongoing risk management.

Penetration Testing Scope

Our testing identifies exploitable weaknesses within web applications, focusing on areas such as:

- Authentication and session management
- Authorisation and access control
- Input validation and data handling
- Configuration and design flaws

Our approach aligns with the [OWASP Top 10 Web Application Security Risks](#), ensuring teams understand critical risks such as injection flaws, broken access control, and insecure design. Testing combines expert manual assessment with tooling to uncover issues that automated scans alone may miss.

Methodology, Process and Reporting

Our structured, risk-based approach ensures consistent, high-quality penetration testing aligned to public sector standards and assurance needs.

1. **Scoping:** We define testing boundaries, objectives, and compliance requirements with stakeholders, including pre-engagement discussions and NDAs to ensure lawful and safe testing.
2. **Planning and setup:** We audit the web application's surface and develop a tailored strategy aligned with your security goals and threat model.
3. **Test execution:** Combining manual expertise and automated methods, testing includes:
 - Intelligence gathering and threat modelling to understand the application's architecture, exposed assets, and likely attack paths.
 - Vulnerability analysis using recognised techniques and tools.
 - Ethically attempt to exploit issues to validate real-world risk without causing disruption.
4. **Reporting and debrief:** we create an encrypted report with an executive summary and technical details covering scope, methodology, identified vulnerabilities, potential impact, and prioritised remediation advice. We provide a debrief to support risk understanding and remediation planning.

Governance and Reporting

In line with the GOV.UK recommendations for handling security test results, our findings are evidence-based, clearly explained, and prioritised by risk to inform both technical and non-technical stakeholders. Encrypted reports are suitable for governance forums, assurance activities, and formal assessments, enabling teams to understand risk in plain language and make informed decisions about mitigation.

Our services support ITHC preparation by helping teams identify weaknesses in advance of formal assurance reviews. Testing is carried out by BPSS-cleared staff, supported by CREST membership and collaboration with CHECK-certified partners to meet recognised public sector assurance expectations.

Vulnerability Assessments

Between penetration tests, we can run automatic periodic vulnerability scans as part of a vulnerability management strategy. Where penetration testing attempts to actively exploit an application through manual attacks, vulnerability scanning uses a cloud-based tool that searches an application for known vulnerabilities.

*Vulnerability scanning is an additional charge to our standard penetration testing service and is only available for web applications.

Other Cyber Security Services

In addition to our Web App Penetration Testing, we provide complementary services to support secure and resilient digital delivery.

They include:

- Mobile Application Penetration Testing - assessing native and hybrid mobile apps across iOS and Android.
- Infrastructure and Network Penetration Testing - identifying vulnerabilities across core IT systems, networks, servers, and connected services before they can be exploited.
- Cloud Configuration Reviews - independent evaluation of cloud environments (AWS, Azure and Google) to identify misconfigurations and strengthen security posture.

Please refer to our other G-Cloud 15 service listings for more information.

04. Assurance and security

We take information security, quality management, and environmental responsibility seriously. Our standards ensure that data is handled securely, confidentially, and in full compliance with regulations, giving public sector teams confidence when handling sensitive information.

We're a CREST member company

We've been a [CREST member company](#) for over 5 years. This demonstrates that our penetration testing services are consistently delivered to the highest security industry standards. For additional cyber assurance, we collaborate with [CHECK-certified](#) partners while maintaining a roadmap to continually enhance our in-house credentials.

We're also certified and committed to:

ISO 27001 - Information Security

Stringent controls to protect sensitive data, including personal and confidential public sector information.

ISO 9001 - Quality Management

A structured quality management system assuring consistent, reliable, and high-quality service delivery.

ISO 14001 - Environmental Management

A commitment to sustainable operations and reducing environmental impact.

Cyber Essentials and Cyber Essentials Plus

UK government-backed certifications demonstrating operational protection against common cyber threats.

Gold Partner - International Software Testing Qualifications Board (ISTQB)

Recognition of our commitment to professional standards and accredited software testing expertise.

BPSS (Baseline Personnel Security Standard)

All Zoonou employees hold BPSS clearance as a minimum, ensuring an appropriate level of assurance for public sector engagements.

For more information on how we handle and process data, including our approach to GDPR compliance, please refer to our [privacy notice](#). Additional details about our policies and certifications are [available on our website](#).

05. Delivery models

We offer a range of QA delivery models, each providing different levels of integration and control to suit your team's size, needs, and project complexity. These models align with common public sector delivery approaches, including agile, waterfall, and hybrid programmes.

Embedded QA

Testers work directly within your existing teams and processes for close collaboration, providing continuous quality insight - ideal for fast-moving agile environments.

Outsourced QA

A fully managed service where we handle all QA activities independently, giving your team clear, actionable results without additional management overhead.

Dedicated QA Team

Long-term partners who become an extension of your team, providing consistent support, deep knowledge of your systems, and continuity across multiple projects.

Project-based QA

Focused, milestone-driven testing for short-term needs such as service launches, feature rollouts, or urgent fixes - perfect for accessing expert support without long-term commitment.

Location and integration

We can deliver QA services:

- Onsite - working directly in your offices to fully integrate with your teams and processes.
- Remote - supporting your team from our offices while maintaining full communication and collaboration.
- Hybrid - flexible mix of onsite and remote delivery to suit your project requirements.

06. Using the service

Pricing

Costs are available in our pricing document.

Availability of trial service

Not applicable for this service.

Ordering and invoicing

To purchase our services, email digitalgov@zoonou.com or call us on [01323 433 700](tel:01323433700).

A statement of work (SoW) will be created to define the scope of the project, deliverables, timelines and cost. Unless otherwise agreed, invoices are issued with 30-day terms, payable by BACS transfer.

We can also assist in completing a call-off contract.

Onboarding

We guide you through getting started with Zoonou efficiently and securely. Our Public Sector team covers:

- Commercial and contractual arrangements, including NDAs.
- Governance, reporting, and escalation routes, ensuring clarity from day one.
- Aligning with your team, tools, and processes to start QA activities smoothly.
- Defining scope, deliverables, and timelines, so expectations are clear for all stakeholders.

Implementation and delivery approach

We embed governance, risk management, and evidence-led assurance throughout every engagement. Our approach is tailored to your team and project requirements, whether supporting sprints, managed QA, or project-based initiatives. This ensures that services are delivered safely, inclusively, and reliably, while protecting operational and citizen-facing outcomes.

Training

Training requirements are defined in individual project SoWs.

Technical requirements and client-side requirements

If applicable, they're defined in individual project SoWs.

After-sales support

We arrange regular review meetings and catch-ups with clients to ensure satisfaction with services and identify any additional support required.

Offboarding

We provide a structured handover at the end of an engagement, leaving teams confident to maintain service quality independently. This includes:

- Final report with findings, actionable recommendations, and next steps.
- Knowledge transfer to strengthen internal QA capability and embed best practices.
- Ongoing support for operational and citizen-facing teams to continue delivering high-quality services.
- Secure closure of project-specific accounts, documentation, and access as required.

Termination process

These are specified in our Terms & Conditions document.

Service constraints

Not applicable for this service.

Backup and restore details

Not applicable for this service.

Service levels

Not applicable for this service.

Data restoration and service migration

Not applicable for this service.

07. Social value

Our social value commitments align with the UK Government's Social Value Model (PPN 002), ensuring every contract we deliver provides measurable social, economic, and environmental benefits beyond our core services.

Tackling economic inequality

We're a Living Wage employer and a [Disability Confident Level 2 organisation](#), actively recruiting, retaining, and developing disabled colleagues. We run a work experience programme for girls aged 14-16, and as "friends" of [Women in Tech Sussex](#), they host meetups in our office, supporting women and non-binary people in tech.

We also support the work of [Tech Resort CIC](#), helping people in our local community who face social disadvantage to access digital skills and improve digital inclusion.

Fighting climate change

We follow ISO 14001 environmental standards and have a carbon reduction plan targeting carbon neutrality by 2030 and net zero by 2050. We use 100% renewable energy, reduce energy wherever possible, and repurpose technology to cut waste.

Through company fundraising, we donate to an environmental charity chosen by our team each year. We also participate in local initiatives such as beach cleans with [Plastic Free Eastbourne](#) and projects rejuvenating local school nature spaces with [Treebourne](#).

Increasing supply chain resilience

We work with local suppliers and B Corp-certified companies wherever possible, building ethical, reliable, and locally connected supply chains.

We keep our supplier base simple, maintain multiple approved suppliers for critical goods, and foster strong relationships through clear communication, planning, and prompt payment, helping suppliers stay financially stable and ready to deliver throughout our contracts.

Building healthier communities

We support local initiatives, including Tech Resort CIC, Treebourne, and Plastic Free Eastbourne, alongside volunteering, workshops, and hands-on activities. Every employee receives two paid volunteer days per year, enabling them to support causes that matter to them personally.

We also donate £10 per employee each year to our [local food bank](#), purchasing and delivering items based on the community's needs. These efforts help make our communities healthier, more inclusive, and environmentally aware.

Driving innovation

We share our expertise through webinars, roundtables, and workshops. Our team regularly speak at client and peer events to promote best practices in QA, accessibility, and digital service delivery.

From 2026, as part of our B Corp commitments, we will also take on pro bono projects supporting organisations that deliver positive social impact.

08. Other QA services

In addition to the services described in this document, we provide a broad range of QA capabilities to meet different needs across the public and third sectors.

This includes accessibility and QA testing for specific sectors (Higher Education, Government, Health/NHS, Charities, Museums/Heritage), cloud migration and system integration testing, ERP/CRM testing, security and penetration testing, load and performance testing, API testing, test automation, and AI/ML assurance.

For more information, [visit our website](#).

09. Contact details

If you work in the public sector and want to explore how Zoonou can support your digital services, our Public Sector team is ready to help.

Rhodri Alexander

Head of Public Sector and Trustee Director

Rhodri leads our Public Sector team; combining deep experience with a practical, hands-on approach, he's been pivotal in shaping our company's services to address the specific needs and challenges of the sector.

You can [connect with Rhodri on LinkedIn](#) and contact our Public Sector team on:

Email: digitalgov@zoonou.com

Tel: [01323 433 700](tel:01323433700)