

DevSecOps audit for cloud-based digital services

Security maturity assessment of DevSecOps capability, delivering strategies and implementation plans to improve agile security practices. Our security experts provide proven methods for incorporating security into agile working practices. We use lightweight, pragmatic approaches, including automation techniques and measurement, which improve security in continuous integration and continuous delivery pipelines.

Our service is recommended for any public sector organisation embarking on cloud technology adoption and usage, with the consequent need to plan for the secure development, testing, deployment and operation of cloud-based digital products and services. It is also recommended for organisations that have existing cloud infrastructure or software in place, but who are concerned with the security practices followed in delivering those services.

Our security consultants carefully analyse existing security practices, for example:

- automated security testing
- threat modelling
- risk analysis
- code review
- static code analysis
- dynamic security testing
- penetration testing
- security monitoring

They then produce guidance and recommendations on how to effectively and efficiently build security into the agile delivery practices of the delivery teams.

We provide a security maturity assessment of DevSecOps capability, delivering recommendations on how to improve agile security practices, leverage continuous delivery to reduce risk and improve the security posture of the organisation. Our security experts provide proven strategies for incorporating security into agile working practices using lightweight and pragmatic approaches, including automation techniques, that measurably improve security in continuous integration and continuous delivery pipelines. Our service helps ensure clients can manage risk effectively within the Shared Responsibility Model of the cloud provider that has been selected.

Our security consultants have in-depth, hands-on experience and expertise in building strong security communities of practice within a diverse variety of organisations and

industries, including government, finance, banking, retail, and many others. Our consultants have first-hand experience in how security works best within agile environments, and how to match corporate security, compliance and risk management with modern iterative delivery practices focused on rapid release to production.

Features

- DevSecOps recommendations based on industry best practices
- Delivers agile security strategy to enhance continuous integration and delivery
- Guides effective vulnerability management
- Identifies individuals in the organisation to lead a security community
- Provides an action plan for implementing security in agile delivery
- Guides adopting and conducting threat modelling
- Assesses the ability to detect and respond to security incidents
- Identifies skills gaps and recommends resourcing plans
- Effective for all cloud platforms, AWS, GCP and Azure

Benefits

- DevSecOps explained by experts using plain English
- Delivered by experienced security consultants
- Proven track record of adopting DevSecOps within government
- Describes how to measure security success meaningfully
- Tailored guidance specific to the delivery programme
- Consultants experienced in meeting GDS and NCSC guidance
- Recommends pragmatic approaches to security
- Improves the quality of external penetration testing exercises
- Drives better decision-making on security budgets
- Identifies security practices that work well with continuous delivery

Our approach to DevSecOps

Equal Experts consultants are highly experienced in modern agile and lean practices. They bring with them experience of a wide range of business domains and industries, including many industries that face strong regulation around security, such as banking and finance. They excel at communicating with senior stakeholders and delivery teams across an organisation, using plain language that is easily understandable to non-security specialists.

Our approach is to assess the maturity of the organisation in building security into software and systems, using industry standards such as the NIST Cybersecurity Framework and OWASP Security Assurance Maturity Model (SAMM), as well as security industry best practices.

Our consultants analyse the current approach to security, identifying any areas of friction between corporate security policies and modern DevOps practices such as continuous integration and continuous delivery. We work with the risk management team to understand the major risks faced by the organisation, alongside common industry risks, and identify any existing security practices that are being followed to respond to those risks.

Once we have a complete picture of the current security practices, we provide an assessment of security maturity and document this based on supporting standards and industry resources, benchmarking the organisation against other similar organisations and industries.

Our security consultants then produce a set of recommendations for DevSecOps practices that should be considered for adoption within the organisation in order to improve security maturity. These recommendations are risk-based and tie directly to measurable security outcomes for the organisation. We do not believe in arbitrary scoring systems, but instead value outcomes that can demonstrably improve security through the reduction of risk. No two organisations are the same, and therefore no two DevSecOps Audit recommendations are the same. The audit recommendations we provide are unique and tailored to the client's particular needs.

We will recommend particular products, where applicable, or certain feature sets that will help deliver more secure services. For example, some organisations do not have a vulnerability management system designed to support continuous delivery or bespoke software development. In cases such as these, we will recommend various approaches to address the gap, either through the procurement of commercial software, the adoption of open source software, or building custom software to address the requirement.

All recommendations are based on products or capabilities that we know to be effective for organisations that have adopted agile delivery techniques and tools. We value automation and integration capabilities, as we believe that many of these features must be tightly integrated into build pipelines in order to be most effective.

Our consultants examine development and operability practices, ensuring that security is considered throughout the lifecycle of the service. We review security monitoring

Making Software. Better.

operations and identify any areas that can be improved in order to bring security and development teams closer together.

As with DevOps, DevSecOps is more about organisational culture and mindset than about any specific technology or technique. A fundamental part of our service is explaining this culture and mindset to all those involved in the delivery of services, from senior management to development teams, in order to give an organisation the best chance of success in secure software delivery.

Examples of DevSecOps in action

A team of Equal Experts security consultants has implemented DevSecOps for a major UK government department, which operates a large microservices architecture running in the cloud, supporting hundreds of microservices. In this example, we have gone beyond the DevSecOps Audit service described earlier and have implemented our own recommendations.

After examining the existing security practices within the department, our security consultants identified a number of areas where improved focus on security would yield measurable benefits to the organisation. We produced a backlog of themes (such as “Application Security”, “Platform Security”, etc.) and epics (such as “Static Analysis”, “Dependency Checking”, etc.) and ranked these based on value to the organisation and security impact. Those items that were determined to have the highest value and impact were tackled first. For example, dependency checking might be a high-value exercise that can be rolled out very quickly with low disruption to delivery teams, yielding great impact in a short space of time; whereas, other epics might require more direct involvement with delivery teams and be slower to roll out with lower impact.

While rolling out improvements in DevSecOps practices across both the platform and the microservices that run on top of it, the team also provided security consulting to delivery teams in order to improve the security capabilities within each delivery team and foster collaboration between security and development. This proved to be an excellent avenue for identifying and encouraging security champions across the organisation, which helped scale the supply of security expertise to better meet demand.

Our team took the lead in security incident response, providing a clear procedure to be followed together with a documented and agreed risk triage framework. This framework provided a barometer for measuring the most appropriate response for a given incident, reducing the tendency to either under- or overreact to security incidents. We also managed the communications between varying stakeholders, including senior

management, delivery teams, corporate security and information risk teams, and the departmental CISO.

The biggest challenge in this project was in scaling supply to meet demand, particularly as we were supporting more than 50 delivery teams working in geographically dispersed locations. To address this challenge, we focused on three main activities:

- Building automated security testing tools that were easy for teams to adopt (or automatically included) in their build pipelines
- Improving platform-level security features, such that all teams and microservices would benefit with little to no change to their services
- Consulting with teams working on higher-risk projects and training them to perform their own threat modelling and security reviews wherever possible

Through these activities, we were able to demonstrate improved security across the platform through:

- Improved day-to-day secure delivery practices followed by teams across all locations
- Improved response time for security incidents, including more thorough and methodical vulnerability analysis and management through to resolution
- Improved security awareness and enthusiastic participation from delivery teams
- Collaborative support between teams on security issues
- Automated, test-driven approach to security vulnerability resolution

Services

We have four core UK-based teams that provide expertise and advice to the organisation, our clients and our partners:

Data and AI

The Data and AI service helps clients make better use of data and create powerful AI solutions that improve and transform any business. We use our deep expertise in data engineering to improve the quality of data that flows through the organisation, providing better insights into customers and operations. Applying our expertise in MLOps, Generative AI, AI in the SDLC and algorithms, we help upskill client teams, automate key services and create new ones.

Design and Product

The Design and Product service helps clients increase adoption and user satisfaction by designing exceptional digital products and services. We use our expertise in user-centred design and product management to discover and solve the most valuable problems, aligned to a client's digital strategy. We help to create delightful customer experiences that deliver real business value, increased user engagement, better brand reputation and additional revenue.

Technology Strategy

Our Technical Strategy service helps teams to confidently navigate the technology landscape and make decisions that will sustain long-term value. Our expertise covers all aspects of technology strategy, including architectural choices, operating model changes and the adoption of emerging technologies. Using our extensive industry and technology experience, we help to plan the practical steps clients need to be ready for the future.

Modernisation and Platforms

Our Modernisation and Platforms service helps to accelerate time-to-value and reduce total cost of ownership, while scaling digital products and systems. Using modern engineering practices, we help to build and run cloud-native services and improve heritage systems. We bring deep expertise in cloud architectures, secure delivery, "you build it, you run it", and platform engineering on AWS, Azure and GCP clouds.

Team

Our core culture and business model prioritise providing value and doing what is best for all our stakeholders, particularly our clients, rather than maximising short-term profits and shareholder returns. Our founders sold the business to an Employee-Owned Trust (EOT) in May 2024 to secure the long-term future of our collaborative approach, highlighting this commitment. The EOT trustees include the founders and representatives of our employees, Associates and clients, ensuring the interests of all stakeholders are considered and balanced in our operations.

Equal Experts is a worldwide network of technology experts who are dedicated to driving innovation. We have Business Units in the UK (London and Manchester), USA, South Africa, Germany, the Netherlands, Australia and India. Our resourcing model is based on a core of permanent senior consultants and a supply chain of 4,000+ carefully selected, expert, independent SME consultants - our Associate network. On a typical engagement,

we pass ~£2 in every £3 of our contract income directly to this network, creating opportunities for entrepreneurship and helping new SMEs to grow.

90% of our consultants have more than 12 years of experience (average more than 18 years) in the development, delivery, operation and maintenance of digital services using agile methods. Many have significantly more and, in some cases, are global influencers, authors and presenters. Their maturity and pragmatism mean they are highly collaborative, happy to transfer knowledge and keen to help clients build internal capability.

We have grown organically, mostly through personal referrals, prioritising quality, experience and cultural fit above all else. After a rigorous selection process, experts are added to our network, whether we need them immediately or in the future.

We select the most suitable people for any contract role from this large pool, not just from a bench of off-charge employees. Our model is resilient and efficient; we form small expert teams, reducing cost and risk for our clients, while achieving outcomes faster than less experienced teams. Our experts train and upskill the whole supply chain, including client staff and those of other suppliers. We have delivered many public and private sector systems (e.g., for HMRC, HMPO, Defra, DWP and MoJ), including CNI, over the past 17+ years using this model. Our approach is data-driven, user-focused and sustainable, allowing us to deliver results quickly and efficiently, using small teams of real experts.

Our standard working model for teams is hybrid remote/on-site, with a core generally based close to client offices, minimising travel costs and environmental impact. This ensures they can be on-site for workshops, meetings and onboarding activities, and can work collaboratively with client team members, stakeholders and other suppliers. In the words of one client, *“your consultants truly leave their Equal Experts badges at the door”*.

Our focus on senior talent means that all our consultants have the skills and experience required to thrive in dynamic, challenging client environments. It means we can focus on work that adds real value, rather than micro-managing more junior consultants. Our non-hierarchical structure also allows us to operate with lower overheads. For our teams, this creates a mature, pragmatic and innovative working environment, where they can implement the best solutions of their already distinguished careers. And for our clients, it translates to better services, delivered faster and at lower overall cost. We were ranked 2nd in Glassdoor’s UK Best Places to Work 2025, up from 4th in 2024, and 15th in Newsweek’s Most Loved Workplaces 2022.

For more information and case studies, please visit <https://www.equalexperts.com/> or contact us at solutions@equalexperts.com.

Making Software. Better.

The information contained in this document is confidential and proprietary. Copyright © 2022-6 Equal Experts. All rights reserved.

Roles

Collectively, our consultants have the multi-disciplinary experience and expertise needed for successful transformation to cloud-first delivery, live service maintenance and new operating models. Our network gives us fast and flexible access to the DDaT skills our clients need. We have specialists in all areas required for digital success, including:

- Delivery managers
- Change managers
- Product managers
- Engagement managers
- Strategic advisors
- Security specialists
- Data scientists
- Data engineers
- Data architects
- Technical leads
- Technical architects
- DevOps consultants
- Developers
- Testers
- Business and performance analysts
- Accessibility experts
- Service designers
- User experience designers
- Content designers
- User researchers

When a client needs specialists or niche skills, we can rapidly and confidently engage with other organisations in our established ecosystem of proven partners. EE interviews each partner consultant to ensure a high level of knowledge and cultural fit before we assign them to clients.

Public sector clients

We're proud to be one of the top suppliers to the public sector via the G-Cloud and DOS frameworks. Our services are also available through RM6190 Technology Services 4, RM6195 Big Data and Analytics (the only supplier on all 6 capabilities), RM6335 DALAS (Lot 2a) and DPS Frameworks including RM3764 Cyber Security 3, RM6173 Automation

Marketplace, RM6094 Spark, RM6200 Artificial Intelligence and RM6235 Space-Enabled and Geospatial Services.

The Equal Experts approach has a successful track record of delivery across the private and public sectors. Some recent award-winning deliveries include:

- HMPO's passport renewal service,
 - ranked #1 public service with a score of 81.2/100 in the July 2025 ICS customer satisfaction survey.
 - Winner of Public Sector Project of the Year and Development Team of the Year at the UK IT Industry Awards 2024.
- HMRC's Data Platform Services Core Engineering Platform, winners of Computing DevOps Excellence Awards 2025 Best Implementation of DevSecOps.
- John Lewis & Partners Best Implementation of DevSecOps at the DevOps Excellence Industry Awards 2023

We know what it takes to implement and support cloud-based applications within complex public sector organisations and across large multi-vendor programmes. We understand and adhere to the GDS digital service standards for delivering solutions and handling and securing data within critical national systems. We have experience in consulting, deploying and supporting security-accredited solutions and have passed numerous GDS assessments. Many of our consultants hold current SC clearance (some have DV) as they have previously worked with public sector clients.

Equal Experts has helped implement digital services to government digital service standards (including passing many formal GDS service standard assessments) for:

- His Majesty's Revenue and Customs (HMRC)
- Department for Environment, Food & Rural Affairs (DEFRA)
- The Home Office and His Majesty's Passport Office (HMPO)
- Ministry of Justice (MoJ), His Majesty's Prisons and Probations Service (HMPPS) and His Majesty's Courts and Tribunals Service (HMCTS)
- Department for Work and Pensions (DWP)
- Department of Health and Social Care (DHSC)
- Department for Business, Energy & Industrial Strategy (BEIS)
- Border Force
- Department for Education (DfE)
- Registers of Scotland
- Office for National Statistics (ONS)
- Intellectual Property Office (IPO)
- States of Guernsey

- Cabinet Office
- Government Digital Service (GDS)
- Valuation Office Agency (VOA)

Planning

To build detailed knowledge of the context and domain for any project, an initial phase of planning, definition and knowledge transfer will generally take place at the start of an engagement.

We have found that this takes place most effectively through a short time-bound inception to develop a shared understanding and agreement on vision and objectives across a broad stakeholder group. This covers the business, technical and user aspects of the project and the outputs may include user personas and scenarios, key user journeys, as-is and desired business processes, a prioritised backlog of user stories, technical constraints and vision, and a release roadmap and plan. The techniques and principles applied are also used on an ongoing basis throughout the course of delivery, to ensure the solutions developed are fit for purpose and meet real and changing user needs.

This initial inception phase can be contracted separately if required.

Setup and migration

In addition to ongoing development and operation of live cloud-based services, we can help with the initial set up and migration as part of a transition to cloud. We look for opportunities to automate processes (for example, test, deploy) that will yield real benefit and high ROI. Our approach helps to address integration, dependencies and risk early. We capture actionable metrics to measure and manage progress towards meeting the agreed success criteria and KPIs identified for building and operating the service. The highly collaborative, interactive processes we follow foster continual learning and improvement of services. They help to establish and evolve the overarching service design, management processes and the team capabilities.

We can ensure projects hit the ground running through our experience in designing, configuring and setup of many continuous delivery and automated cloud deployment environments. These techniques allow software to be repeatably and reliably deployed and tested through each stage into production on the cloud. We have substantial experience when it comes to the tooling required for continuous delivery and automated software deployment, greatly facilitating the software set up, build and migration process, which increases programme productivity and reduces project risk and cost.

Quality assurance and performance testing

We hold ISO9001:2015 Quality Management System certification. All our consultants have extensive experience in both manual and automated testing, including performance testing, continuous integration and delivery into production environments at scale. With all clients, we actively encourage the adoption of robust and meaningful automated test coverage, delivery and test techniques, to reduce risk and safely increase delivery velocity. We are happy to work with a client's existing quality management system (QMS) where appropriate.

Security services

We hold ISO27001:2022 Information Security Management System, Cyber Essentials and Cyber Essentials Plus certifications.

We can provide the following security services if required:

- Security strategy
- Security risk management
- Security design
- Security incident management
- Security audit services

Training

For every client, we aim to transfer and embed knowledge of technology and process innovation. Our consultants have the expertise, skills and enthusiasm to help transfer knowledge of new technologies and ways of working to our clients' team members, upskilling staff and helping to build their internal delivery competence and capability. This improves internal competencies and builds long-term sustainable capability, as clients migrate to modern cloud-based products and services. We tailor particular practices to address specific organisational constraints – we recognise that every organisation is different and there is no “one size to fit all”.

We tend not to offer classroom-based training as our consultants are happy to share their knowledge throughout a project. They take responsibility for helping individual client team members adopt new practices and ways of working.

Ongoing support

Our operational philosophy is “you build it, you run it”. The delivery team responsible for the development of a live service usually also takes responsibility for its operation. We have found that development teams which support their own products are motivated to deliver higher quality, more robust and maintainable code.

When a service is live with real users, we expect the delivery team to provide 2nd line (infrastructure, in conjunction with hosting support agreements) and 3rd line (applications) support during business hours. We can agree on an appropriate model for 24/7 on-call coverage if required - see our G-Cloud On-Call Support offering for details. We typically establish an on-call rota with delivery team members assigned weekly.

Our experience is that digital services are never really finished and that it is important to retain some level of investment to allow the addition of new features as the needs of customers (both internal and external) change. Our design of the end-to-end service can include establishing Service Level Agreements for ongoing service evolution and operational support (ensuring agreed levels of service availability).

User support

We provide an engagement manager on all G-Cloud engagements with responsibility for ensuring clients objectives are met and for addressing any issues with service delivery. Our engagement managers act as an escalation point and can be reached via phone or email to respond to issues beyond the control of the team providing the service. Engagement management is included within our service pricing.

When a service is live with real users, we expect the delivery team to provide 2nd-line (infrastructure, in conjunction with hosting support agreements) and 3rd-line (applications) support during business hours, within the agreed service cost. We can agree on an appropriate model for 24/7 on-call coverage if required - see our G-Cloud On-Call Support offering for details. We typically establish an on-call rota with delivery team members assigned weekly.

Social Value, the Environment and CSR

Our values and ethos extend beyond our organisation and people, and we take our corporate social responsibility seriously. We are committed to working with all our clients to share our knowledge and learnings, and contribute to their CSR goals, e.g. we will

Making Software. Better.

The information contained in this document is confidential and proprietary. Copyright © 2022-6 Equal Experts. All rights reserved.

facilitate discussions with their designated digital sustainability leads, to collaborate on environmental policy goals, discuss current practices for greening software and agree enhancements aligned with industry policies, like the Greening Government Strategy.

We willingly collaborate closely with our clients, other suppliers, competitors and the wider ecosystem to discuss, share and test innovative environmental and social value ideas and initiatives, to improve sustainable practices and create added value throughout any contract.

We will follow our proven social value methodologies for any G-Cloud 15 contract, aligned with the UK's Public Services (Social Value) Act 2012, PPN002 (PA2023) and the Social Value Model, and the UN Sustainable Development Goals, to actively create additional opportunities to develop, measure and improve social value for our client and their entire supply chain. In a recent [Government Transformation Magazine interview](#), Mike Potter, ex-UK Gov CDO recalled his HMRC experience partnering with us for transformative results. *"We didn't just buy their capability - we bought their culture,"* he said. *"Cultural alignment is key. When you pick partners who share your values and ways of working, you find areas of mutual advantage."*

We review, update and publish our Carbon Reduction Plan, Modern Slavery and EDI statements annually, are a Disability Confident employer, a member of the Business Disability Forum and a participant in the Government Digital Sustainability Alliance (GDSA). Our commitment to providing a fulfilling workplace for everyone is reflected in Glassdoor's Best Places to Work in the UK, voted for by our staff, ranking us 4th in 2024, 2nd in 2025.

We complete the [EcoVadis](#) assessment tool, which evaluates performance across four dimensions: Environment, Labour and Human Rights, Ethics and Sustainable Procurement. We complete the assessment, create an improvement plan and review and update it annually. We willingly share the results with clients and use their feedback and learnings to influence our improvement plans.

Examples of other social value initiatives for clients include:

HMRC Joint Value Initiatives: we work closely with HMRC to organise and fund JVs, e.g.:

- [School visits](#) to encourage children to pursue STEM careers & find future data engineers,
- Data Engineering Academy - supporting HMRC to onboard and upskill new starters and develop their technical expertise through bootcamps and placements on EE projects,

- Hosting the [Women in Tech & Leadership Conference 2025](#) in collaboration with HMRC's Women in Tech Network.

Hace: We co-funded a [project](#) to develop an AI-based data analysis tool to objectively quantify a company's Child Labour performance.

Médecins Sans Frontières (MSF): We staffed a pro bono project to build the [Malaria Anticipation Project \(MAP\)](#), deployed in Lankien, South Sudan and being planned for Anka, Nigeria.

John Lewis: We shifted to lower-footprint GCP cloud data centres in Switzerland to meet JL's environmental sustainability goals.

Government: We are an active member of the Government Digital Sustainability Alliance ([See more details here](#)) and are actively working with Defra to implement exemplar projects such as:

- Implementing Green coding Standards ([See Version 1 Github](#)) in our teams working with Defra to help support learnings for wider Government.
- Working with Defra and our partner [Heata](#) to develop an innovative decentralised cloud compute project. The aim is to reduce the carbon footprint of cloud workloads by 80% and heat farmers' domestic water tanks to save them money.