Mastek™

Trust. Value. Velocity

G-Cloud 14

Cloud DevSecOps Consultancy Service

Contents

1. About Mastek

Mastek has been delivering Critical National Infrastructure programmes in the UK Public Sector for over a decade now. We are trusted with multiple contracts for the UK Government across Central Government, Health, Local Government, Policing, Public Protection, and Defence. The majority of our national services are delivered in a context of high uncertainty and complexity while collaborating in multi-supplier environments.

While working for these large and complex public sector organisations, we have continuously refined our management, delivery and underlying processes to reflect key learnings from the sector:

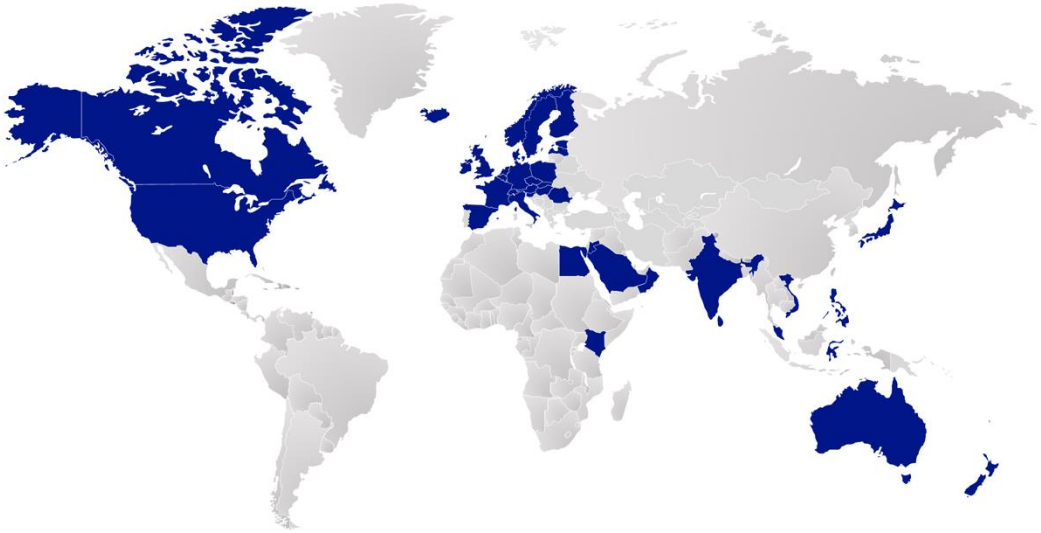
Working through a complex stakeholder landscape: We understand the importance of establishing effective communication channels, building trust, and fostering a collaborative working environment that empowers stakeholders to contribute meaningfully to the project's success. Our approach is based on a deep understanding of stakeholder needs and requirements. We leverage our experience and expertise to design governance structures that promote transparency and accountability and use data-driven reporting mechanisms to ensure stakeholders have real-time visibility into project status and progress. At the Home Office, GDS, Ministry of Defence and NHS, we have a proven track record of working seamlessly with large stakeholder groups, including civil servants.

Standards, compliances: We comply with >20 policies and standards, including Government Digital Standards and Government CDDO Service Toolkit covering service standards, service manuals, TCoP, API technical and data standards. Our stringent governance, methods, playbooks, and processes (manual and automated) span across service delivery phases, ensuring continuous compliance.

Policy-driven: Policies and procedures largely drive Public Sector organisations. We need to be Agile and flexible to meet demands for policy/regulatory changes, geopolitical events, and ministerial commitments.

Culture: We adhere to the Civil Service core values of integrity, honesty, objectivity, and impartiality. Key behaviours we promote stem from a combination of Civil Service and Mastek values. These include being passionate, accountable, sustaining predictable and repeatable outcomes, not transferring risk, transparent, leading to enable, acting with transparency, practising a no-blame culture, and being flexible.

Mastek's global presence



Australia
Austria
Bahrain
Belgium
Brunei
Canada
Denmark
Egypt
Estonia
Finland
France
Germany
Hungary
Iceland
India
Indonesia
Ireland
Italy
Japan
Jordan
Kenya
Kingdom of Saudi Arabia (KSA)
Kuwait
Latvia
Luxembourg
Malaysia
Netherlands
New Zealand
Norway
Oman
Philippines
Poland
Romania
Singapore
Slovakia
Spain
Sri Lanka
Sweden
Switzerland
United Arab Emirates (UAE)
United Kingdom
USA

Mastek
Trust. Value. Velocity

Did you know?

75%

Around three quarters of Local Authorities in the UK who run Oracle have worked with Mastek on their digital transformation journey.

300,000 Users

Supported managing up to 750,000 logins per month to MOD though Identity and Access Management

Crime reduction

We designed, built and manage the UK's Strategic National DNA Database that helps Forensics and Law Enforcement Authorities investigate & stop crime

90% faster

We enabled the National Health Service (NHS) to drive 90% faster response times with a billion pharmacy prescriptions a year.

Technical Service Desk

We provide level 2 and ITSM support for the One Login service at Government Digital Service

22k

Our systems enable 22,000 schools to function efficiently every day of the year.

Healthcare and manufacturing

We delivered Finance, HCM & Supply Chain transformations for clients across health and manufacturing globally powered by Oracle Cloud

Transformation of trade

Transforming UK's trade with the EU and rest of the World by supporting Customs Declarations Services and its trade users.

99.99% Availability

We support the Home Office Biometrics (HOB) Platform, Having migrated it to an AWS platform.

Our digital and cloud services portfolio

Powered by Glide 4.0 and value-based delivery

Industry-aligned approach with business outcomes

Digital engineering and experience	• Cloud engineering & migration • Legacy modernisation • Low code / no code App Dev • DevSecOps • Enterprise integration	• MACH • Digital commerce • UX & CX • Platform engineering • Gen AI software development.
Oracle Cloud and enterprise apps	• Oracle Cloud applications • Oracle consulting • Oracle Cloud infrastructure	• Value-based delivery • Glide 4.0.
Data, automation and AI	• Cloud data modernisation • Business Intelligence & Analytics	• Data management • Intelligent automation • Data Governance.
Salesforce	• Sales Cloud • Service Cloud • Marketing Cloud • Industry Cloud	• Experience Cloud • Mulesoft.
Innovation labs and platforms	• Enterprise workforce scheduler • Connected enterprise • icx-Pro – intelligent part assistant	• iLeaseFinPro.
Cloud enhancement managed services	• Oracle managed services • Digital managed services • Commerce managed services	• Salesforce managed services.

Home Office Biometrics (HOB)

Public sector platform modelled 24x7 with 99.99% availability

Problem

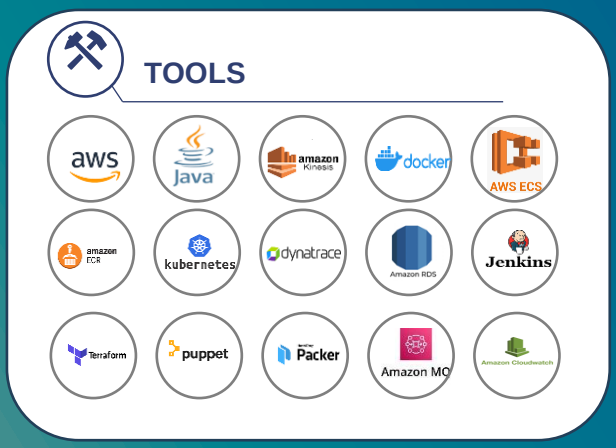
- Transition business-critical Platform services from incumbent supplier with minimal risk
- Migration from private cloud to AWS Cloud.

Solution

- Migrated the infrastructure from private cloud to AWS
- Embedding Kubernetes Containerisation
- Introduced Docker and fully-baked AMIs
- Supporting the platform's self-service functionality using Jenkins Jobs
- Applying security updates to the OS base images through pipelines
- Instituting automated patching and testing for infrastructure images
- Support of configuration, test, and releasable artefacts through the pipeline.

Outcome

- **Zero impact** on live service
- **80% automation** of SIT
- Environment Provision **2 days to 1 hour**
- **5x scalability** in handling student BRPs
- Cost saving the authority circa **£9.5m/year.**
- Won the **'Best Use of Cloud Services'** award
- **35%** Incident Volume Reduction.



Government Digital Service

Problem

GDS initiated the One Login programme to create a single front door for identity verification and authentication, which could be adopted and scaled across all government departments. This would improve the user experience by providing the public with a single identification and verification service for the government, reduce costs as each department no longer required its own identity service, and reduce identity fraud and identity-enabled crime.

GDS released a tender in June 2023 to provide a Technical Service Desk (TSD) managed service for the One Login service. This service would provide a single point of contact for level 1 and 2 service support as part of the wider support ecosystem. It would be provided in the UK and replace the incumbent's scaled-down non-ITIL-aligned break-fix service.

Solution

In September 2023, Mastek were successfully awarded the TSD contract to deliver TSD on behalf of GDS. GDS had an extremely aggressive programme driven by the onboarding of HMRC as a user, which was a major milestone planned for February 2024, migrating new and existing HMRC users to the One Login platform. The TSD service was expected to go live in November 2023. This was an extremely complex programme which, within this timescale, would deliver:

- The contact centre provider for level 0 directly facing the public
- The TSD supplier in place directly facing all government departments
- The TSD supplier in place providing L1 and L2 engineering support and monitoring
- Continued delivery on the One Login backlog of features
- Continued migration of smaller government departments to the platform.
- Delivery of a new ITSM toolset to be configured for use by GDS and the One Login programme, integrating level 0 to level 3 support
- Working as one team, Mastek quickly integrated into the programme, appointing the leadership team early in the engagement. We collaborated with GDS from the outset, ensuring we tailored the service to their expectations rather than delivering what was written in the contract.

  Our leadership team consisted of:

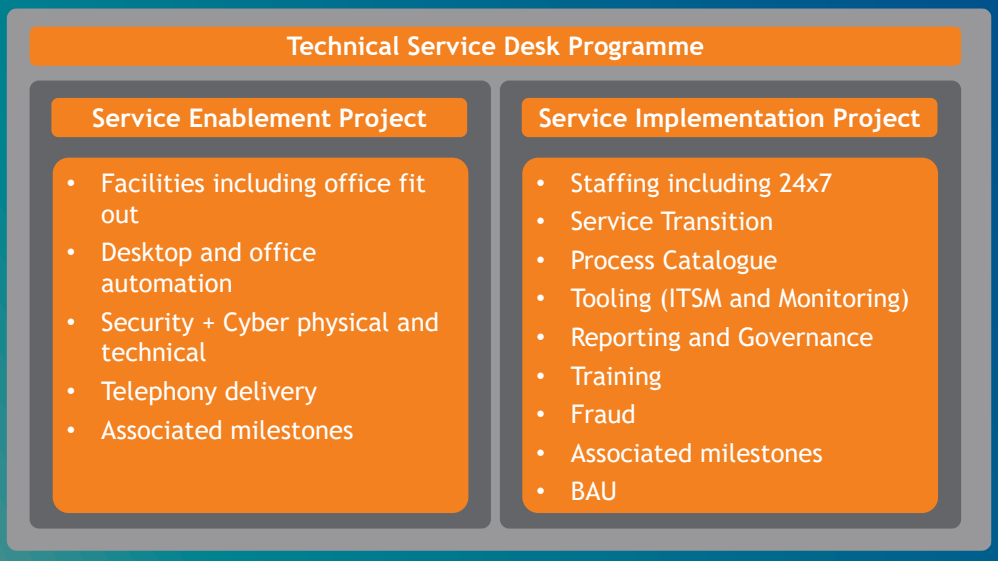
  - Service Management Vice President
  - Programme Director
  - Chief Technology Officer
  - Programme Management office lead.

Outcome

At its height, the programme team was circa 15 strong, covering programme/project delivery, PMO, architecture, fraud, security, support, omni channel and quality assurance. The service team is currently in place providing circa 21 resources now covering end-to-end service management, service delivery and L1 and 2 engineering roles.

As the One Login migrations continue, Mastek is supporting Government departments onboarding to the platform as they transition into the new service and provide One Login a secure Technical Service Desk managed service with:

- Omni channel access for other government departments via telephony, email and web form
- Provision of L1 and L2 engineering support
- 24x7, 365 days a week cover
- 24x7x365 eyes on monitoring service
- Fraud detection and security, GDPR compliant
- End-to-end (L0-3) incident and problem management
- End-to-end 24x7 Major incident management (MIM)
- On-call/call-out engineering support, incident and MI management
- Adherence to stringent SLAs on incident response, call handling and fix times
- End-to-end monthly service reporting alongside TSD KPI and SLA reporting.
- A shift left culture and mindset, reducing the impact of service on product teams (L3)
- Support with service maturity in the programme, preparing GDS to run critical national infrastructure.



Internet-facing platform & applications for Army Digital Services

Developed mobile app & web app with 24*7 high availability

Problem

- New Defence Gateway Portal
- Combine all internet-facing applications into one
- Easy to use
- Enable easier access to the MySeries portfolio of products.

Solution

Designed and developed the following easy-use Progressive Web Apps:

- Defence Gateway Landing Page
- My Leave App
- My Expenses App
- My Health App
- My Details App
- My Appraisal App
- My Admin App
- COVID-19 Reporting Tool
- Commanders' COVID-19 Tool.

Outcome

- Delivered 20+ successful projects
- Deployment Automation
- £7.5m in savings annually
- Zero Downtime
- Environment creation in hours.

Delivered a platform for the Department for Health and Social Care

Delivered capability supporting 200k+ tests in a day, traced millions of COVID-19 infections

Problem

- Leveraging DevOps platform based on reusable GitHub, AWS, and Azure DevOps Pipelines
- Introduce more flexible, scalable, and reusable IaC capabilities
- Implement CI/CD pipelines.

Solution

- Uplifted from Cloud Formation into Terraform (IaC)
- Pre-built the AMIs using Packer, with automated security checks
- Immutable infrastructure, thus eliminating the risks of partial upgrades and patches
- Continual Cost Optimisation processes and other service functions, such as Change and Risk management
- Migrated into an organisation-wide collaboration toolset. This included Jira, Confluence, Trello, Miro, Teams, SharePoint, O365, Slack, etc.

Outcome

- 75% reduction in lead time due to pre-built AMIs
- Zero Downtime Deployments
- Delivered a Platform - Secured, multi-tenanted hosted on Azure and AWS in 5 weeks
- Cost reduction achieved through close monitoring of resource utilisation.

Mastek and Technology in the Public Sector

Technical Capabilities	Relevant Technology Capability	Mastek Scale
Software Development Continuous Integration, Platform - Other Products, Cloud Collaboration Tools		**Software Engineering 2354 FTE**
QA and Test; API, Automated Functional and Compatibility, Accessibility & Performance		**QA and Testing 774 FTE**
Cloud Platforms Amazon Web Services AWS Microsoft Azure		**Cloud Platforms 1046 FTE**
Data BI/MI Components, Integration		**BI and Visualisation 725 FTE**
User-Centered Design		**UCD 25 FTE**
Office Automation Tools		**Collaboration 4565 FTE**

2. DevOps and DevSecOps

DevOps/DevSecOps is a cultural and professional movement that sprang up in response to mistakes commonly made by large organisations. Often, these organisations have separate units for development, quality assurance, and operations business and in extreme cases, these units may be based in various locations, work for different organisations, or have entirely different management structures. Communication costs between these units and their individual incentives lead to slow delivery and a mountain of interconnected processes. This is what DevOps aims to correct. It is not a methodology or framework but a set of principles.

DevOps focuses primarily on improving collaboration and communication between Development (Dev) and Operations (Ops) teams to streamline the software delivery process. The primary goals of a DevOps approach include accelerating the delivery of software, increasing deployment frequency, and achieving faster time to market. It achieves this by fostering a culture of collaboration, transparency, and shared responsibility across development and operations teams, with an emphasis on automation, Continuous Integration, Continuous Delivery (CI/CD), and infrastructure-as-code (IaC) to enable faster and more reliable software delivery.

DevSecOps extends the principles of DevOps by integrating security practices into the software development lifecycle alongside development and operations. It emphasises a proactive approach to security rather than treating security as an afterthought or a separate stage. By embedding security considerations throughout the software development lifecycle, from design and development through to deployment and operation, it enables organisations to build and deploy secure, resilient, and compliant software at scale, improving agility and delivering higher-quality software products faster.

DevOps, and more specifically, DevSecOps, are an essential part of enabling a cloud-based project to achieve the highest levels of efficiency, quality, and effectiveness.

A high-level view of the DevSecOps lifecycle is detailed in Figure 1 below:

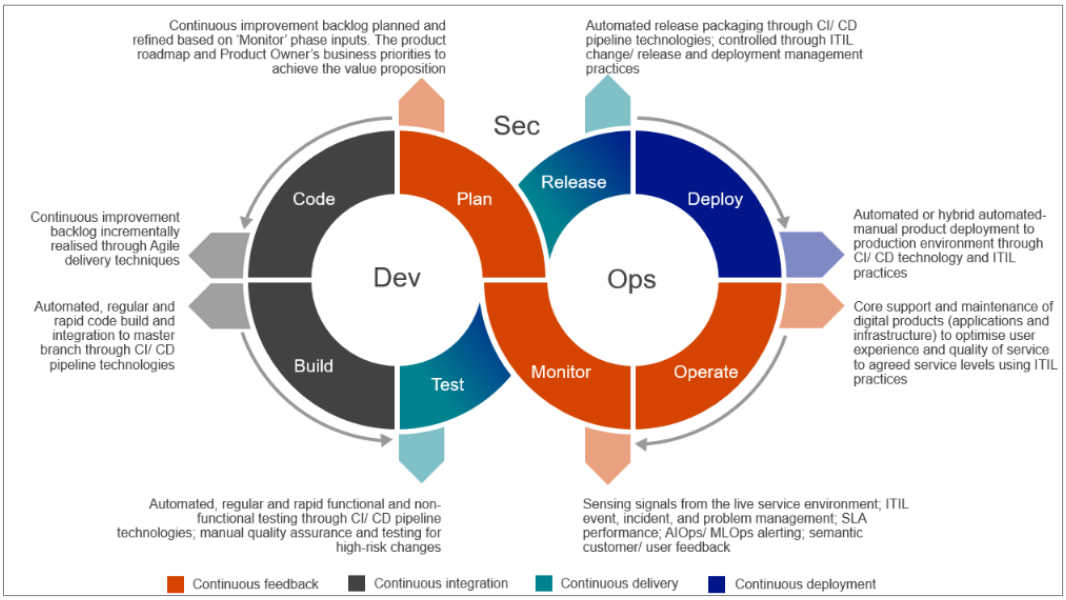


Figure 1: Mastek's DevSecOps

DevSecOps is not just about technology:

- **Culture**: DevSecOps needs a change in attitude, so shared ownership and collaboration are key to building and managing a service.
- **Process automation**: Many business processes are ready to be automated. Automation removes manual, error-prone tasks, allowing people to concentrate on the quality of the service. Areas benefiting from automation are:
  - Release management (releasing software)
  - Provisioning
  - Configuration management
  - Systems Integration
  - Monitoring
  - Orchestration (the arrangement and maintenance of complex computer systems)
  - Quality assurance/testing.
- **Measurement**: By defining a set of key metrics and measuring and monitoring performance against them throughout the software development lifecycle, your organisation is best placed to measure success and embrace a culture of continuous improvement. Example metrics are deployment frequency, security vulnerabilities, compliance adherence, time to remediate, mean time between failure, mean time to detect, and mean time to respond.
- **Sharing**: People from diverse backgrounds (i.e. development and operations) often have different but overlapping skill sets. Sharing information between groups spreads an understanding of the different areas behind a successful service, so encourage it. Resolving issues will then be more about working together and not negotiating contracts.

3. Key Components

The key components of DevSecOps include various practices, tools, and cultural aspects that aim to integrate security into the software development lifecycle.

Culture and collaboration

- **Shared responsibility:** Encourages a culture where everyone, including developers, operations teams, and security professionals, shares responsibility for security.
- **Cross-functional teams:** Promotes collaboration and communication among development, operations, and security teams, breaking down silos and fostering a collective approach to security.
- **Security awareness training:** Provide ongoing training and education to raise awareness about security best practices and threats across the organisation.

Automation

- **Continuous Integration/Continuous Deployment (CI/CD):** Automates the process of building, testing, and deploying software, enabling rapid and reliable delivery while integrating security checks at every stage.
- **Infrastructure as Code (IaC):** Automates the provisioning and configuration of infrastructure using code, allowing for consistent and secure deployment environments.
- **Automated security testing:** Integrates automated security testing tools into the CI/CD pipeline to identify vulnerabilities, assess risks, and enforce security policies early in the development process.

Security practices and tools

- **Static Application Security Testing (SAST):** Analyses source code for security vulnerabilities and coding errors before deployment.
- **Dynamic Application Security Testing (DAST):** Tests running applications for security vulnerabilities by simulating real-world attacks.
- **Container security:** Implements security measures for containerised applications, including image scanning, runtime protection, and secure configuration.
- **Secrets management:** Safely stores and manages sensitive information such as (Application Programming Interfaces (API) keys, passwords, and cryptographic keys.
- **Compliance automation:** Automates compliance checks and ensures adherence to regulatory standards and security policies throughout the development lifecycle.

Continuous monitoring and feedback

- **Security monitoring:** Implements real-time monitoring and logging to promptly detect and respond to security incidents.
- **Vulnerability management:** Tracks and prioritises security vulnerabilities, ensuring timely remediation and continuous improvement of security posture.
- **Incident response:** Establishes procedures and tools for responding to security incidents effectively, minimising their impact on the organisation.

Risk management and compliance

- **Risk assessment**: Identifies and assesses security risks associated with software applications and infrastructure, prioritising mitigation efforts based on risk severity.
- **Compliance management**: Ensures compliance with regulatory requirements, industry standards, and internal security policies through automated compliance checks and documentation.

4. Business Benefits

DevSecOps integrates security practices into the DevOps process, enabling organisations to deliver secure, high-quality software products efficiently while reducing risks and maximising business value. As such, it offers several key business benefits:

- **Improved security**: By integrating security practices early in the software development lifecycle, DevSecOps helps identify and address security vulnerabilities sooner, reducing the likelihood of security breaches and data leaks. This proactive approach enhances the organisation's overall security posture.
- **Compliance and regulatory alignment**: DevSecOps helps organisations meet compliance requirements and regulatory standards by integrating security and compliance checks into the development pipeline. This ensures that applications and systems adhere to industry regulations and standards, reducing the risk of non-compliance penalties.
- **Enhanced collaboration**: DevSecOps promotes collaboration and communication among development, operations, and security teams. By breaking down silos and fostering a culture of collaboration, organisations can leverage the collective expertise of cross-functional teams to address security challenges effectively.
- **Increased customer trust**: With security integrated throughout the development process, businesses can demonstrate their commitment to protecting customer data and privacy. Enhanced security measures instil trust and confidence in customers, leading to stronger customer relationships and brand loyalty.
- **Faster time to market**: DevSecOps streamlines the development process by automating security testing and compliance checks, allowing teams to detect and fix security issues quickly. This agility results in faster release cycles, enabling businesses to deliver new features and updates to customers more rapidly, gaining a competitive edge.
- **Cost savings**: Identifying and addressing security vulnerabilities early in the development process is more cost-effective than fixing them after deployment. DevSecOps minimise the potential impact of security breaches, reducing the financial losses associated with data breaches, regulatory fines, and reputational damage.
- **Continuous Improvement (CI)**: DevSecOps promotes a culture of CI by emphasising automation, feedback loops, and iterative development. By continuously monitoring and refining security practices, organisations can adapt to evolving threats and vulnerabilities, ensuring ongoing protection against security risks.

5. Mastek's Service

Mastek provides a complete set of consultancy services, which, combined with other techniques (including solution value mapping, incremental strategy, uncertainty management and emergent design), help to ensure that cloud-based solutions meet the Government Digital Service (GDS) Digital by Default standard. We cover everything from an initial DevSecOps Readiness Assessment through the transition itself into running and enhancing your DevSecOps processes.

This means we can take care of everything from defining the workflows, selecting and configuring tooling, automating processes, monitoring and reporting, day-to-day operations, and continuous improvement.

Some of the areas covered by our consultancy services:

- DevSecOps readiness assessment
- DevSecOps transformation
- Process mapping (collaboration and workflow)
- Process improvement/automation
- Monitoring and reporting (continuous improvement)
- Performance assessments
- Tooling:
  - Tool selection (Terraform, Cloud Foundry, Open Stack etc.)
  - Implementation
  - Configuration management
  - Environment provisioning
  - Continuous Integration and Deployment (CI/CD)
  - Process-automation
  - Test-automation.

DevSecOps Readiness Assessment (DSORA)

Mastek provides a tailored assessment based on your current processes and practices. The assessment looks at all aspects of your organisation's Software Development Life Cycle (SDLC), identifies opportunities for improvement, and assesses your ability to implement and sustain change. This assessment then lays the foundation for developing a roadmap for implementing and maturing your DevSecOps capabilities.

1. Organisational culture and leadership:
   - Evaluate the organisation's culture regarding collaboration, agility, and innovation.
   - Assess leadership support for DevSecOps initiatives.
   - Identify any cultural barriers to adopting DevSecOps practices.
   - Is funding available to support the transition
2. Team structure and skills:
   - Determine if teams are cross-functional and have the necessary skills for DevSecOps.

- Identify gaps in skills related to security, automation, and collaboration.
- Assess the effectiveness of communication and collaboration among teams.

3. Processes and workflows:
   - Review existing development and operations processes and workflows.
   - Evaluate how security is integrated into each stage of the SDLC.
   - Identify opportunities to automate the development and operations processes including how to incorporate security checks and tests.
4. Tools and infrastructure:
   - Assess the current development, testing, and deployment toolset.
   - Evaluate the availability of security tools for vulnerability scanning, static code analysis, etc.
   - Identify any gaps in tooling needed to support DevSecOps practices.
5. Security policies and compliance:
   - Review existing security policies and procedures.
   - Ensure that DevSecOps practices align with regulatory requirements and industry standards.
   - Identify any compliance risks associated with the adoption of DevSecOps.
6. Risk management:
   - Assess the organisation's risk management processes.
   - Identify potential security risks in the development and deployment pipeline.
   - Determine how risks are monitored and mitigated throughout the SDLC.
7. Metrics and measurement:
   - Define key performance indicators (KPIs) for measuring the effectiveness of DevSecOps initiatives.
   - Establish benchmarks and targets for security, quality, and delivery speed.
   - Determine how metrics will be tracked and reported to stakeholders.
8. Training and education:
   - Provide training and education for teams on DevSecOps principles and best practices.
   - Offer specialised training for development, operations, and security professionals on automation and collaboration tools.
   - Encourage continuous learning and knowledge sharing within the organisation.
9. Continuous Improvement (CI):
   - Establish a culture of continuous improvement and learning.
   - Encourage feedback from teams and stakeholders to identify areas for improvement.
   - Implement regular retrospectives to reflect on successes and challenges.

Our DSORA has been used by many private, public, and not-for-profit organisations to help them develop a coherent strategic roadmap for adopting DevSecOps.

DevSecOps Transformation

Our DevSecOps Transformation services help transition software development and operations within an organisation to a DevSecOps Model. Assisting you with both business and technical change consultancy.

--- End of Document ---

Mastek UK Ltd.
100 Brook Drive, Green Park,
Reading, Berkshire
RG2 6UJ
+44 (0)118 903 5700

Email: g-cloud@mastek.com