



Trust. Value. Velocity

## G-Cloud 15

Cybersecurity CTEM-Based Vulnerability  
Remediation Service

**Contents**

|    |                                    |    |
|----|------------------------------------|----|
| 1. | About Mastek .....                 | 3  |
| 2. | Summary.....                       | 13 |
| 3. | Key Features.....                  | 14 |
| 4. | Business Benefits .....            | 15 |
| 5. | Tools and Framework Services ..... | 16 |

## 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 contexts of high uncertainty and complexity, while collaborating across 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, the Ministry of Defence, and the NHS, we have a proven track record of working seamlessly with large stakeholder groups, including civil servants.

**Standards, compliance:** We comply with >20 policies and standards, including Government Digital Standards and the Government CDDO Service Toolkit, covering service standards, service manuals, TCoP, and 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

## 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 through 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 and 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 and 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

|                                           |                                                                                                                                                                                                                  |                                                                                                                                                                                   |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Digital engineering and experience</b> | <ul style="list-style-type: none"> <li>• Cloud engineering and migration</li> <li>• Legacy modernisation</li> <li>• Low code / no code App Dev</li> <li>• DevSecOps</li> <li>• Enterprise integration</li> </ul> | <ul style="list-style-type: none"> <li>• MACH</li> <li>• Digital commerce</li> <li>• UX and CX</li> <li>• Platform engineering</li> <li>• Gen AI software development.</li> </ul> |
| <b>Oracle Cloud and enterprise apps</b>   | <ul style="list-style-type: none"> <li>• Oracle Cloud applications</li> <li>• Oracle consulting</li> <li>• Oracle Cloud infrastructure</li> </ul>                                                                | <ul style="list-style-type: none"> <li>• Value-based delivery</li> <li>• Glide 4.0.</li> </ul>                                                                                    |
| <b>Data, automation and AI</b>            | <ul style="list-style-type: none"> <li>• Cloud data modernisation</li> <li>• Business Intelligence and Analytics</li> </ul>                                                                                      | <ul style="list-style-type: none"> <li>• Data management</li> <li>• Intelligent automation</li> <li>• Data Governance.</li> </ul>                                                 |
| <b>Salesforce</b>                         | <ul style="list-style-type: none"> <li>• Sales Cloud</li> <li>• Service Cloud</li> <li>• Marketing Cloud</li> <li>• Industry Cloud</li> </ul>                                                                    | <ul style="list-style-type: none"> <li>• Experience Cloud</li> <li>• Mulesoft.</li> </ul>                                                                                         |
| <b>Innovation labs and platforms</b>      | <ul style="list-style-type: none"> <li>• Enterprise workforce scheduler</li> <li>• Connected enterprise</li> <li>• icx-Pro – intelligent part assistant</li> </ul>                                               | <ul style="list-style-type: none"> <li>• iLeaseFinPro.</li> </ul>                                                                                                                 |
| <b>Cloud enhancement managed services</b> | <ul style="list-style-type: none"> <li>• Oracle managed services</li> <li>• Digital managed services</li> <li>• Commerce managed services</li> </ul>                                                             | <ul style="list-style-type: none"> <li>• Salesforce managed services.</li> </ul>                                                                                                  |

# 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 and applications for Army Digital Services

Developed mobile app and 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                            |
|-------------------------------------------------------------------------------------------------------------|--------------------------------|-----------------------------------------|
| <b>Software Development</b><br>Continuous Integration, Platform - Other Products, Cloud Collaboration Tools |                                | <b>Software Engineering</b><br>2354 FTE |
| <b>QA and Test:</b> API, Automated Functional and Compatibility, Accessibility & Performance                |                                | <b>QA and Testing</b><br>774 FTE        |
| <b>Cloud Platforms</b><br>Amazon Web Services AWS<br>Microsoft Azure                                        |                                | <b>Cloud Platforms</b><br>1046 FTE      |
| <b>Data BI/MI</b><br>Components, Integration                                                                |                                | <b>BI and Visualisation</b><br>725 FTE  |
| <b>User-Centered Design</b>                                                                                 |                                | <b>UCD</b><br>25 FTE                    |
| <b>Office Automation Tools</b>                                                                              |                                | <b>Collaboration</b><br>4565 FTE        |

## 2. Summary

Mastek will deliver **CTEM-based remediation** management as a managed, outcomes-led service that continuously reduces exposure by running a repeatable cycle of scope-setting, discovery, prioritisation, validation and mobilisation, turning findings into measurable risk reduction, not just more vulnerabilities to track.

The service will stand up governance, remediation SLAs, ownership and reporting, then operationalise remediation by integrating prioritised work into ITSM/change workflows (for example, using remediation task states and workflows) so fixes are driven through to closure with auditable evidence. It will be run as a continuous programme (not a one-time project), with ongoing prioritisation tuning, remediation blocker removal and regular stakeholder reporting to demonstrate risk reduction over time.

The service covers consulting to agree on the CTEM scope (critical assets, priority services and key threat vectors) and to define governance, remediation SLAs and reporting outcomes that business and technology leaders can use. Implementation then onboards exposure sources, establishes continuous discovery and builds a prioritisation model that highlights which exposures most contribute to risk against critical assets, rather than treating all findings as equal. Validation activities confirm exploitability and control effectiveness using an attacker-perspective approach, ensuring effort is targeted on issues that genuinely change risk.

Mobilisation operationalises remediation by creating trackable tasks, assigning owners and integrating work into ITSM/change workflows so fixes are executed and evidenced through to closure. Managed operations to sustain the programme by tuning prioritisation, removing operational blockers, driving remediation cadence and continuously demonstrating posture improvement over time.

### 3. Key Features

- Define Scope covering assets, projects and threat vectors.
- Establish continuous discovery exposures across the in-scope attack surface.
- Risk-based prioritisation using business context, exploitability and attack-path impact.
- Validation of exposures and control effectiveness.
- Mobilise remediation by tracking and enforcing SLAs.
- Integrate with ITSM-style remediation workflows and change processes.
- Create remediation tasks and maintain an auditable state.
- Produce executive and operational reporting.
- Establish runbooks for exceptions, compensating controls and risk acceptance.
- Ongoing managed operations to tune prioritisation, drive continuous improvement.

#### 4. Business Benefits

- Shrink the remediation backlog by focusing on exposures.
- Improve accountability by assigning ownership and tracking outcomes.
- Reduce wasted effort by validating exploits before remediation.
- Reduced TCO and increased coverage of remediation.
- Provide a consistent, executive-friendly remediation plan.
- Remediation aligned with NIST-SP-800-40r4.
- Reduce the window of opportunity for attackers.

## 5. Tools and Framework Services

Tools:

- CTEM-based solution: XMCyber, Rapid7, Qualys, Tenable, covering a five-stage cycle: scoping, discovery, prioritisation, validation, mobilisation
- NIST SP 800-53 Revision 4 security control baseline, including RA-5 (Vulnerability Scanning) and CA-7 (Continuous Monitoring) for exposure discovery and continuous oversight.
- CIS Controls – Continuous Vulnerability Management (for continuous identification, prioritisation and remediation discipline).
- MITRE ATT&CK (to map exposure and remediation priorities to adversary tactics/techniques and validate what matters).

--- 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](mailto:g-cloud@mastek.com)

