



SERVICE DEFINITION DOCUMENT

*QA, Testing & Test
Automation*

73 Church View, Hollywood,
BT18 9LN – United Kingdom
+44 (0)2890 394 431
info@cranmo.re



Contents

1. Purpose of this Document	3
2. Service Description	3
2.1 Overview.....	3
2.2 Service Components	3
2.3 Service Benefits	4
3. Delivery Approach.....	5
3.1 Test Strategy & Planning	5
3.2 Test Framework Development	5
3.3 Test Execution & Automation.....	5
3.4 Continuous Testing Integration.....	6
4. Service Constraints	6
5. Security and Compliance	7
5.1 Security Accreditations	7
5.2 Testing-Specific Security	7
6. Pricing	7
7. Contact Information	8

1. Purpose of this Document

This document provides comprehensive information about Cranmore's QA, Testing & Test Automation service and how it is delivered to public sector organisations through the G-Cloud 15 framework.

This Service Definition is required as part of Cranmore Consulting's application to provide services to the public sector via the G-Cloud framework, in accordance with Crown Commercial Service requirements.

The content and structure of this document aligns with the guidance published by the Crown Commercial Service for G-Cloud 15 service providers.

2. Service Description

2.1 Overview

Cranmore's QA, Testing & Test Automation service provides comprehensive quality assurance and testing capabilities for public sector digital services. Our independent testing approach ensures applications, systems, and digital platforms meet the highest standards of quality, security, accessibility, and performance.

We combine manual testing expertise with advanced test automation frameworks to deliver efficient, thorough testing across the software development lifecycle. Our service covers functional and non-functional testing, including performance, security, accessibility, and API testing, ensuring compliance with government digital standards.

Our qualified testing engineers work collaboratively with development teams, embedding testing within Agile and DevOps workflows to accelerate delivery while maintaining quality. We provide test strategy, test planning, test case development, test automation through technologies such as Playwright, and continuous testing capabilities that align with GDS Service Standards and public sector requirements.

2.2 Service Components

Our QA, Testing & Test Automation service includes:

- **Test Strategy Development:** Comprehensive test strategies aligned with project objectives, risk assessments, and compliance requirements for public sector environments.
- **Test Planning & Management:** Detailed test plans, test case design, test data management, and test environment configuration using industry-standard tools and methodologies.
- **Functional Testing:** Thorough validation that applications meet functional requirements, including user acceptance testing (UAT), integration testing, and regression testing.
- **Test Automation Frameworks:** Implementation of robust test automation using leading frameworks including Playwright, and custom automation solutions.
- **Performance Testing:** Load testing, stress testing, scalability testing, and performance monitoring to ensure systems handle expected user volumes and peak demands.
- **Security Testing:** Penetration testing, vulnerability scanning, security audits, and compliance verification against government security standards (Cyber Essentials Plus).
- **Accessibility Testing:** Comprehensive WCAG 2.2 AA compliance testing, assistive technology testing, and accessibility audit services ensuring inclusive digital services.

- **API Testing:** RESTful API testing, API security testing, and API performance testing using specialised tools.
- **Continuous Testing:** Integration of automated tests within CI/CD pipelines, enabling rapid feedback and shift-left testing approaches in Agile environments.
- **Mobile Testing:** Testing across iOS and Android platforms, including responsive design testing, mobile app testing, and cross-device compatibility verification.
- **Regression Testing:** Automated regression test suites that verify existing functionality remains intact after changes, updates, or new feature implementations.
- **Test Data Management:** Creation, management, and maintenance of test data sets, including synthetic data generation and data privacy considerations.
- **Defect Management:** Comprehensive defect tracking, prioritisation, reporting, and lifecycle management using tools such as JIRA.
- **Test Reporting & Metrics:** Detailed test execution reports, quality metrics dashboards, defect trend analysis, and test coverage reporting for stakeholder visibility.
- **Quality Assurance Consultancy:** Expert advice on testing strategy, quality processes, test maturity assessment, and QA best practices for public sector digital services.

2.3 Service Benefits

Benefits of Cranmore's QA, Testing & Test Automation service include:

- **Enhanced Quality:** Independent testing provides objective quality validation, identifying defects early and ensuring digital services meet user expectations and requirements.
- **Reduced Risk:** Comprehensive testing coverage reduces the risk of production failures, security vulnerabilities, and accessibility issues that could impact service users.
- **Accelerated Delivery:** Test automation and continuous testing enable faster release cycles while maintaining quality standards, supporting Agile and DevOps practices.
- **Cost Efficiency:** Early defect detection is significantly more cost-effective than addressing issues in production, reducing remediation costs and service disruption.
- **Compliance Assurance:** Testing verifies compliance with government digital standards, WCAG accessibility requirements, and security standards (Cyber Essentials, GDPR).
- **Improved User Experience:** Thorough functional and usability testing ensures digital services are intuitive, reliable, and meet user needs across all scenarios.
- **Performance Confidence:** Performance testing validates system capacity and scalability, ensuring services remain responsive under expected and peak loads.
- **Security Validation:** Security testing identifies vulnerabilities before deployment, protecting sensitive government data and maintaining public trust.
- **Accessibility Compliance:** Dedicated accessibility testing ensures digital services are inclusive and meet legal requirements.
- **Repeatable Quality:** Automated test suites provide consistent, repeatable testing that scales with project growth and enables efficient regression testing.
- **Continuous Improvement:** Test metrics and reporting provide data-driven insights for quality improvement and informed decision-making throughout the project lifecycle.

Flexible Engagement: Our testing services scale to project needs, providing dedicated testing teams, embedded testers, or consultancy support as required.

3. Delivery Approach

QA, Testing & Test Automation engagements typically involve the following activities depending on project scope:

3.1 Test Strategy & Planning

The testing foundation is realised through collaborative discovery, requirements analysis, and strategic planning. Our testing team works with stakeholders to understand project objectives, identify testing scope, assess risks, and define quality criteria.

Key activities include:

- **Requirements Analysis:** Review functional and non-functional requirements, user stories, and acceptance criteria
- **Test Strategy Definition:** Develop comprehensive test strategy covering approach, scope, resources, and timelines
- **Risk Assessment:** Identify testing risks, quality risks, and mitigation strategies
- **Tool Selection:** Evaluate and select appropriate testing tools, automation frameworks, and test environments
- **Test Planning:** Create detailed test plans specifying test types, test cases, test data, and success criteria
- **Environment Setup:** Configure test environments, establish test data sets, and prepare testing infrastructure

3.2 Test Framework Development

This involves building the test automation framework, developing test cases, and preparing test environments. Our engineers implement robust automation architectures that support maintainable, scalable test suites aligned with the application technology stack.

Key activities include:

- **Test Case Development:** Design and document comprehensive test cases covering functional and non-functional requirements
- **Automation Framework Setup:** Implement test automation frameworks (such as Playwright) with best practice architecture
- **Test Script Development:** Develop automated test scripts with appropriate assertions, validations, and error handling
- **Test Data Preparation:** Create test data sets, synthetic data, and test data management processes
- **Integration Configuration:** Configure test automation integration with CI/CD pipelines and version control systems
- **Performance Test Setup:** Prepare performance testing scenarios, scripts, and monitoring configurations

3.3 Test Execution & Automation

The test execution phase involves running comprehensive test suites, identifying defects, validating fixes, and refining automation coverage. Testing activities align with development sprints in Agile environments, providing continuous quality feedback.

Key activities include:

- **Functional Testing:** Execute functional test cases validating all application features and user journeys
- **Automation Execution:** Run automated test suites across multiple browsers, devices, and configurations
- **Performance Testing:** Conduct load tests, stress tests, and scalability assessments measuring system capacity
- **Security Testing:** Perform security scans, penetration testing, and vulnerability assessments
- **Accessibility Testing:** Validate WCAG 2.2 AA compliance using automated tools and manual assistive technology testing
- **Defect Management:** Log, track, prioritize, and verify defects through resolution and retest cycles
- **Regression Testing:** Execute regression test suites verifying existing functionality after code changes
- **Test Reporting:** Provide daily test execution reports, defect summaries, and quality metrics dashboards

3.4 Continuous Testing Integration

This embeds testing within the continuous integration and delivery pipeline, enabling automated quality gates and supporting ongoing development. We establish sustainable testing practices that maintain quality as the application evolves.

Key activities include:

- **CI/CD Integration:** Fully integrate automated tests into CI/CD pipelines with appropriate quality gates
- **Test Optimization:** Refine test suites for efficiency, removing redundancy and improving execution speed
- **Knowledge Transfer:** Train development and operations teams on test frameworks, test execution, and maintenance
- **Documentation:** Provide comprehensive test documentation, runbooks, and maintenance guides
- **Handover Support:** Support transition to BAU with guidance on ongoing test maintenance and expansion
- **Continuous Improvement:** Establish quality metrics monitoring and continuous improvement processes

4. Service Constraints

The following constraints apply to this service:

- **Test Environment Access:** Testing requires access to appropriate test environments that replicate production configurations
- **Requirements Quality:** Testing effectiveness depends on clear, complete, and testable requirements documentation
- **Test Data Availability:** Access to representative test data (or ability to create synthetic data) is required for comprehensive testing
- **Tool Licensing:** Some commercial testing tools may require separate licensing arrangements by the Buyer
- **Scheduled Maintenance:** Planned service improvements and framework updates are communicated 30 working days in advance
- **Urgent Changes:** Critical security updates or defect fixes may be implemented inline with agreed SLA notice periods
- **Resource Availability:** Testing resources are scheduled based on agreed engagement terms and may require notice for scaling

5. Security and Compliance

5.1 Security Accreditations

Cranmore maintains:

- **ISO 27001** – International standard for information security management
- **Cyber Essentials Plus** – Independently verified cyber security controls
- **Security Clearance (SC)** – Key personnel hold UK Security Check clearance enabling work with OFFICIAL and OFFICIAL-SENSITIVE data

5.2 Testing-Specific Security

All testing activities adhere to government security standards and data protection requirements. Test data is handled in accordance with GDPR and UK data protection legislation. Security testing follows NCSC guidance and all relevant standards. Test environments are isolated from production systems, and all test artifacts containing sensitive data are securely disposed of at engagement conclusion. Our testing personnel undergo security screening appropriate to the classification of systems under test.

6. Pricing

Pricing for this service is based on:

- **Engagement Scope:** Pricing reflects the scope of testing required, system complexity, and number of test cycles
- **Duration:** Costs scale with engagement duration
- **Resource Requirements:** Pricing considers the testing team size, seniority, and specialist skills required

Detailed pricing is provided following discovery and requirements analysis. All prices are exclusive of VAT.

See pricing documents for more information.

Document Version: 1.0

Last Updated: January 2026

7. Contact Information

Primary Contact

Fergus McGrath
Sales Director
Cranmore Consulting
Mobile: 07912 777717
Email: fergus@cranmoreconsulting.com

Service Desk

Telephone: 028 9042 1238
Email: info@cranmoreconsulting.com

Registered Office

Cranmore Consulting Ltd
73 Church View, Holywood
BT18 9LN
United Kingdom

G-Cloud 14 Listing

<https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/479964968691217>