



Service Definition Document

September 2026

Supplier (via Reseller): XMA Ltd
Subcontractor / SaaS Provider: Tricentis GmbH
Lot: 2a – Infrastructure SaaS (I-SaaS)
Framework: RM1557.15 – G-Cloud 15

1. Service Definition	3
2. Service Features.....	4
3. Service Benefits	6
4. Integrations / Extensions	7
5. Service Scope and Dependencies	9
6. Service Constraints	11
7. Service Levels and Support	12
8. Onboarding / Offboarding.....	14
9. Accessibility.....	15
10. Data Protection and Security	15
11. Backup and Disaster Recovery	19
12. Pricing and Commercial Information	19
13. Ordering Information	19
14. Supplier Information	20
15. Tricentis Contact Information	20

Copyright 2025 Tricentis GmbH. All rights reserved. No part of this document may be reproduced, stored in, or introduced into a retrieval system or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Tricentis . Tricentis is pleased to submit this proposal in response to Crown Commercial Service's Request for the G-Cloud 15 Framework. Statements in this proposal regarding characteristics of products and services are based on our current understanding of Crown Commercial Service's requirements and environment. Such statements are provided for informational purposes; they are believed accurate but not warranted. In our experience, it is common for requirements to evolve somewhat and for understanding of the environment to grow between the time of the proposal's response submission and contract execution. If there is a need for certain technical or performance characteristics to become contractual requirements, we understand that such requirements will be identified and may be incorporated into the statement of work and/or contract prior to agreement execution

1. Service Definition

Tricentis provides cloud-based continuous testing and quality assurance solutions that accelerate digital transformation and ensure application reliability across enterprise systems. The platform integrates with major technologies—including SAP, Salesforce, Oracle, ServiceNow, and CI/CD pipelines—to automate testing, improve performance, and reduce release risk.

The following SaaS products are included in the Tricentis G-Cloud 15 offering, in addition the offerings are also optionally available to be installed on customer premises and/or private cloud infrastructure, please contact Tricentis for further information:

- **Tosca** – Model-based automated testing across UI, API, and mobile.
- **Data Integrity** – Automated data validation and reconciliation across complex systems.
- **qTest** – Centralized test management with real-time reporting and DevOps integration.
- **NeoLoad** – Performance and load testing for scalable applications.
- **LiveCompare** – SAP change impact analysis and intelligent test optimization.
- **SeaLights** – AI-driven quality intelligence for continuous delivery pipelines (SaaS only).

Tosca – Service Definition

Tricentis Tosca is a cloud-based automated testing solution that enables public sector organisations to test applications across web, desktop, mobile, and API interfaces. Tosca uses model-based automation to reduce manual testing effort, accelerate release cycles, and improve test coverage across mission-critical and enterprise applications, including SAP, Salesforce, Oracle, and custom systems.

Data Integrity – Service Definition

Tricentis Data Integrity automates the validation of data accuracy, completeness, and consistency across complex systems and integrations. It enables organisations to detect data discrepancies early across transformation pipelines, source systems, and reporting layers. The service helps ensure trustworthy data for regulatory, operational, and analytical use across public sector environments.

qTest – Service Definition

Tricentis qTest is a SaaS test management platform that enables teams to plan, track, execute, and report on testing activities in one central location. It integrates with common development and DevOps tooling, helping public sector teams collaborate efficiently, maintain testing governance, support Agile delivery, and improve visibility across software programmes.

NeoLoad – Service Definition

NeoLoad is a performance and load testing solution designed to help organisations validate system scalability and reliability before deployment. It enables automated performance testing of APIs and enterprise systems such as SAP and Salesforce. Public sector teams use NeoLoad to identify bottlenecks earlier and ensure mission-critical applications meet service expectations.

LiveCompare – Service Definition

LiveCompare provides automated change impact analysis for SAP landscapes. It analyses planned system changes and identifies the functions, processes, and integrations most at risk. This enables organisations to focus testing effort where it matters, reduce regression workloads, and support safer, more predictable SAP upgrades, releases, and migrations.

SeaLights – Service Definition

SeaLights is a quality intelligence platform that analyses test coverage, code changes, and release risk across development pipelines. It enables organisations to optimise test prioritisation and reduce unnecessary testing effort. The service helps public sector teams improve confidence in releases, support continuous delivery practices, and maintain software quality at scale.

2. Service Features

Tosca – Service Features

Tosca provides model-based automated testing across web, mobile, desktop, packaged applications, and APIs. It supports functional, regression, end-to-end, and risk-based testing within the same platform. Tosca enables test automation using reusable components, allowing non-technical and technical users to build tests without scripting. The solution includes test data management, distributed execution, test portfolio optimisation, and automation for SAP, Salesforce, Oracle, ServiceNow, and custom applications. Tosca integrates with CI/CD pipelines to support continuous testing workflows.

Data Integrity – Service Features

Data Integrity enables automated validation of data accuracy, completeness, lineage, and transformation across complex enterprise systems. It tests data from source systems through middleware, integration layers, and reporting platforms to ensure data quality at every stage of processing. The service supports automated schema comparison,

reconciliation, business rules validation, anomaly detection, and tracking of system-to-system data movement. Data Integrity integrates with data warehouses, ETL tools, cloud data platforms, and ERP systems including SAP, Oracle, and Snowflake.

qTest – Service Features

qTest is a test management platform that centralises test assets, execution tracking, and reporting in one interface. It supports manual, automated, and exploratory testing and provides structured workflows for backlog management, defect handling, and release planning. qTest integrates with Jira, Azure DevOps, CI/CD tooling, and automation frameworks to support Agile and DevOps delivery models. Features include permissions management, audit trails, automated test scheduling, dashboards, and analytics for traceability and governance across delivery teams.

NeoLoad – Service Features

NeoLoad provides performance, load, and scalability testing for modern and legacy applications. It supports protocol-level testing and real-browser testing against APIs, web applications, mobile applications, and enterprise platforms including SAP and Salesforce. NeoLoad enables automated script generation, test design reuse, simulated user behaviour modelling, and dynamic test execution environments. The service includes dashboards for performance monitoring, capacity reporting, and failure diagnostics, and integrates with CI/CD and observability platforms to support continuous performance testing.

LiveCompare – Service Features

LiveCompare automates SAP change impact analysis, enabling organisations to identify which business processes, integrations, and custom objects are affected by updates or configuration changes. The service analyses SAP transports, system usage data, custom code, and test libraries to determine testing priorities. LiveCompare includes dependency mapping, risk scoring, change simulation, and recommendations for regression scope. It integrates with Tricentis Tosca and qTest to support automated test selection and execution based on SAP system change data.

SeaLights – Service Features

SeaLights provides software quality intelligence and test optimisation by analysing code changes, test coverage, and release risk. It collects data from pipelines, test frameworks, source repositories, and build systems to determine where testing should be focused. Features include coverage mapping, change-based testing analytics, readiness scoring, trend analysis, and integration with automation and CI/CD environments. SeaLights

supports a wide range of programming languages, frameworks, and cloud-native delivery models to enable continuous testing decisions.

3. Service Benefits

Tosca – Service Benefits

Tosca helps organisations reduce reliance on manual testing by enabling automated execution of tests across applications and interfaces. Automation helps shorten release cycles, improve repeatability, and reduce the risk of defects entering production. The model-based approach enables faster maintenance of test coverage when applications change, supporting continuous delivery and large-scale enterprise transformation programmes. Tosca supports cross-application testing, which enables departments to validate integrated systems and ensure consistent behaviour across multiple platforms.

Data Integrity – Service Benefits

Data Integrity helps ensure the accuracy and trustworthiness of data used in reporting, operational decision-making, and citizen-facing services. Automated validation helps identify issues early in data pipelines, reducing the likelihood of data-related defects being discovered late in delivery or after deployment. The service supports compliance with internal data governance policies by providing auditable checks and repeatable validation processes. It enables teams to identify quality gaps and improve confidence in data used for regulatory, analytical, and operational purposes.

qTest – Service Benefits

qTest provides centralised visibility of testing activities across teams and projects, enabling stakeholders to track progress, risk, and coverage. It supports efficient collaboration between testers, developers, and business teams by providing shared workflows and consistent processes. By integrating with Agile and DevOps tools, qTest helps organisations coordinate testing across iterative delivery cycles and improve governance and traceability. This helps organisations maintain auditability, support compliance frameworks, and manage testing at scale.

NeoLoad – Service Benefits

NeoLoad helps organisations assess how applications perform under expected and peak workloads before deployment. Identifying bottlenecks and performance risks early helps prevent service disruption and supports resilient system operation. Automated test execution supports repeatability and reduces the effort required for performance validation across releases. The service helps internal teams understand capacity requirements,

system behaviour, and scalability considerations for enterprise and public-facing platforms.

LiveCompare – Service Benefits

LiveCompare helps organisations prioritise SAP testing based on the areas most affected by planned changes. This reduces the need for broad regression cycles by focusing effort where risks are highest. By analysing transport activity, system usage, and configuration changes, the service helps reduce time required to prepare for releases and upgrades. This supports safe delivery of SAP change programmes and helps minimise unplanned downtime or disruption to business operations.

SeaLights – Service Benefits

SeaLights enables change-based testing by identifying the parts of a system most impacted by recent development activity. This helps teams optimise test execution and reduce the volume of testing required while maintaining confidence in release readiness. The service provides insight into testing completeness, helping teams identify gaps and improve resource allocation. This supports more efficient release cycles and helps organisations maintain software quality as delivery frequency increases.

4. Integrations / Extensions

Tosca – Integrations and Extensions *

Tosca integrates with a wide range of enterprise applications including SAP, Salesforce, Oracle, ServiceNow, and web-based platforms. It supports automation across multiple interfaces such as UI, API, and mobile applications. Tosca also integrates with CI/CD pipelines using tools such as Jenkins, Azure DevOps, and GitHub Actions. The platform can be extended through reusable testing components, shared object libraries, and connectors that support automated testing within large enterprise system landscapes.

Data Integrity – Integrations and Extensions *

Data Integrity integrates with a variety of data platforms including SAP, Oracle, SQL databases, Snowflake, cloud data warehouses, and ETL tools. It supports connectivity to structured datasets, reporting systems, and transformation pipelines to enable end-to-end data validation. The service can also work alongside existing data governance, reporting, and analytics platforms, enabling automated checks across multiple stages of the data lifecycle. Optional configuration is available to support integration with Customer-managed authentication and security controls.

qTest – Integrations and Extensions *

qTest integrates with major Agile and DevOps platforms including Jira, Azure DevOps, GitHub, and CI/CD systems. It supports automated testing frameworks and testing tools including Tricentis Tosca and third-party solutions. The platform can be extended to align with existing programme governance processes through workflows, permissions, and reporting dashboards. These integrations help consolidate test management and enable consistency across development, testing, and release cycles.

NeoLoad – Integrations and Extensions

NeoLoad integrates with CI/CD tools such as Jenkins, Azure DevOps, and GitLab to support automated performance testing as part of delivery pipelines. It supports scripting and protocol-based testing for enterprise systems including SAP, Salesforce, and custom applications. The platform can be used alongside monitoring tools and observability platforms, enabling teams to analyse performance behaviour and track system responsiveness under varying load conditions. Optional plug-ins and connectors are available for integration with automation environments.

LiveCompare – Integrations and Extensions

LiveCompare integrates with SAP systems including SAP ECC, SAP S/4HANA, and SAP Solution Manager. It collects information from transport records, usage data, configuration, and custom code repositories to determine the scope and impact of system changes. LiveCompare can also connect with Tricentis Tosca and qTest to support prioritised regression testing based on identified changes. Integration may require suitable SAP permissions and secure connectivity to the Customer SAP environment.

SeaLights – Integrations and Extensions

SeaLights integrates with build and deployment pipelines, test automation frameworks, and source code repositories. Supported integration points include Jenkins, GitHub, Azure DevOps, and other CI/CD tools. The platform works alongside automated and manual testing activities to analyse testing completeness and release risk. Customers may extend the service through plug-ins, SDKs, or pipeline configuration, enabling use in multiple delivery environments and programming languages where applicable. Integrates with Jenkins, GitHub, Azure DevOps.

* Please Note; Additional Add-On capabilities may need to be purchased and licensed to extend and integrate the above. Please contact Tricentis for further information.

5. Service Scope and Dependencies

Service Scope

This service provides access to cloud-based software applications delivered as Software as a Service (SaaS). The service includes platform access, maintenance, security patching, and feature updates as part of the subscription. The scope includes configuration within the platform, integration enablement where available, and the ability to manage users, roles, and permissions. The service also includes documentation, online learning materials, and access to standard support channels as defined in the Support section of this Service Definition.

The service does not include bespoke development, implementation consulting, custom integration development, or local device configuration unless otherwise agreed through a separate engagement outside of the G-Cloud framework. Where optional onboarding or enablement activities are required, these must be arranged under a separate Statement of Work (if applicable).

Service Dependencies

Use of this service requires the following minimum technical dependencies:

- A stable internet connection with corporate-approved network access to SaaS endpoints.
- A supported modern web browser (such as Microsoft Edge or Google Chrome).
- Valid user authentication credentials and applicable roles assigned by the Customer.
- Where API or CI/CD integration is enabled, suitable access permissions and configuration must be provided.

For services that support integrations with third-party platforms (such as SAP, Oracle, Salesforce, Jira, Azure DevOps, Jenkins, or testing frameworks), configuration and enablement of those environments remain the responsibility of the Customer. Some services may require optional on-premises connectors or secure integration agents, which must be deployed and maintained within the Customer environment if chosen.

If internal firewalls, proxy rules, or access controls restrict communication from the SaaS platform or connector to the Customer environment, the Customer remains responsible for making the necessary configuration changes.

Customer Responsibilities

The Customer is responsible for:

- Ensuring licensed users comply with the published product terms and acceptable use policy.
- Providing and maintaining suitable access credentials, MFA (where required), and role-based permissions.
- Ensuring their infrastructure, systems, and devices meet minimum technical requirements.
- Configuring integrations and APIs where required for use of the service.
- Managing organisational security controls, including identity management and endpoint security.
- Maintaining data accuracy, compliance ownership, and retention policies for data stored or processed in the service.
- Ensuring appropriate internal governance for user provisioning, access control, and auditing.

The Customer must also ensure that any content uploaded, processed, or stored within the service complies with applicable policies, regulatory requirements, and statutory obligations including UK GDPR, Freedom of Information Act (FOIA), and local security classifications.

Where Customer systems or configuration prevent intended operation (including browser extensions, restricted access, unsupported versions, or incompatible environments), remediation is the responsibility of the Customer.

Additional Notes by Service

Service	Additional Scope Notes (only if applicable)
Tosca	Local execution engines or automation hosts may be required for specific environments such as desktop UI automation or controlled networks.

Service	Additional Scope Notes (only if applicable)
Data Integrity	Access to source and target systems, datasets, schemas, and service accounts may be required for automated data reconciliation.
qTest	Integration with Jira, Azure DevOps, GitHub, or automation tools requires Customer access tokens or configuration.
NeoLoad	Load-testing against Customer applications may require performance test environments, test data, and agreed traffic scenarios.
LiveCompare	SAP connectivity requires correct authorisation levels, RFC access, transport data, and SAP landscape mapping.
SeaLights	Build pipeline integration requires installation of CI/CD plugins or SDK use where applicable.

Out of Scope

The following are not included unless separately contracted:

- End-user training beyond standard documentation and online learning resources.
- Custom integrations or development work.
- Testing services performed by Tricentis personnel.
- Infrastructure hosting outside the SaaS offering.

6. Service Constraints

This service is delivered as Software as a Service (SaaS) and operates within the parameters of the platform's design. The service must be accessed through a supported web browser and an internet connection that meets the minimum connectivity requirements. Availability may be subject to planned maintenance windows, which are scheduled where possible outside UK business hours and communicated in advance. Emergency maintenance may occur if required to maintain service stability or security.

Certain features may require configuration by the Customer, including integrations with third-party systems, secure agent deployment, or use of automation frameworks or connectors. Where integrations rely on Customer-managed platforms or infrastructure, the Customer is responsible for access rights, authentication configuration, and compliance with policies relating to those systems.

Service performance may depend on Customer infrastructure, network configuration, and the characteristics of applications or data under test. The service does not provide bespoke configuration, custom development, or testing consultancy unless separately agreed. Functionality delivered as part of the service may evolve over time as part of the supplier's product roadmap.

Optional add-ons or extensions may require separate enablement or licensing depending on the selected service tier.

7. Service Levels and Support

Support Model and Service Level Agreement (SLA)

Support Model

Support for this service is provided remotely as part of the subscription. Customers may contact support through the online support portal or email. The support service includes access to knowledge base articles, product documentation, release notes, and technical resources. Users with appropriate permissions may raise, track, and manage support cases through the portal.

The support service is designed to assist with platform usage, configuration queries, and fault resolution. Support does not include custom configuration, consulting, training, or professional services unless separately contracted through the reseller (XMA). Support is provided in English.

Support Availability

Severity 1 tickets receive an initial response within 2 hours, 24 × 7, including weekends.

Severity 2 issues are answered within 6 business hours.

Severity 3 within 12 business hours; these business-hour targets apply Monday–Friday, so lower-severity questions logged at the weekend are handled at the start of the next business day.

Incident Categories and Response Targets

Incidents raised by Customers are categorised according to severity and business impact. Response targets are measured from the point the incident is logged within supported hours.

Severity Level	Description	Target Response Time
Severity 1 (Critical)	Complete service outage or critical functionality unavailable with no workaround.	< 2 hours
Severity 2 (High)	Major functionality impaired or issue significantly impacts operations; workaround available.	< 6 hours
Severity 3 (Medium)	Partial loss of functionality or non-critical service impact.	< 12 hours

Resolution times may vary depending on issue complexity, third-party dependencies, and Customer environment configuration.

Maintenance and Planned Service Interruptions

Planned maintenance windows are used for upgrades, security updates, and platform improvements. Where possible, maintenance will occur outside UK business hours.

Customers will be notified in advance of:

- Planned outages
- Major updates
- Changes that may require Customer configuration adjustments
- Emergency maintenance may occur without prior notice where needed to protect service availability or security.

Service Availability Commitment & Service Credits

We guarantee at least 99.0 % monthly availability for our SaaS products, calculated each subscription month as (total minutes – downtime) ÷ total minutes, with scheduled maintenance (notified 48 hours in advance) and force-majeure events excluded. If this target is not met, we automatically issue service credits applied to the customer's next subscription invoice, and Platinum Support customers may instead apply equivalent credits toward their support renewal.

Availability guarantees and related credits do not apply to customer-hosted deployments such as Tosca or LiveCompare, where infrastructure uptime is under the customer's control.

Customer Responsibilities for Support

To enable effective support, Customers are responsible for:

- Providing accurate information and reproduction steps
- Assigning an internal technical contact or administrator
- ensuring users operate supported browser and environment versions.
- managing third-party integration credentials and access
- testing changes in appropriate non-production environments before deployment

Support cannot be provided for environments, configurations, or integrations that are outside supported system requirements.

Service Versioning and Updates

The service is maintained and updated as part of the standard subscription. For Cloud deployments product enhancements, security patches, and functional updates are applied automatically with no need for Customer installation. Release notes and change information are communicated in advance where applicable. Updates may introduce improvements, new features, or modifications to existing functionality, and may require configuration adjustments by the Customer for dependent integrations or automation workflows.

Service Status and Reporting

System status information, planned maintenance notifications, and service updates are communicated through the support portal. Customers may access documentation, release information, and technical updates through the portal as part of their subscription. Incident and ticket reporting related to service performance or availability is also available through the support portal, subject to applicable roles and permissions.

8. Onboarding / Offboarding

Onboarding is delivered remotely and includes provisioning of the service, administrator account setup, and access to product documentation and support resources.

Customers are responsible for user configuration, permissions, and integration setup according to internal requirements.

At contract end, customers can self-service export their data before scheduled deletion.

For qTest, all requirements, test assets, and defects can be exported in CSV, Excel, HTML, PDF, or via the REST API, and the tenant remains available for 60 days before data is erased.

NeoLoad Web SaaS keeps the tenant accessible for 30 days so customers can download test results and reports; backups are retained for a further 30 days before deletion.

SeaLights and LiveCompare provide bulk-export capabilities (for example, JSON REST endpoints) for all analytics or analysis datasets, while Tosca data resides in the customer's own environment, allowing export or backup through existing enterprise tools at any time.

Offboarding includes the ability for Customers to export their data in standard formats before the end of the subscription. Access will remain available for a limited period solely to facilitate data extraction. After this period, the environment and associated data will be deleted in line with documented retention and sanitisation processes. Optional offboarding assistance may be requested if required.

9. Accessibility

This service is designed to be usable by a wide range of users and follows accessibility considerations aligned with recognised accessibility design principles. Where applicable, the service aims to support compliance with the Web Content Accessibility Guidelines WCAG 2.2 AAA, EN 301 549 standard. Accessibility documentation, including product accessibility statements or Voluntary Product Accessibility Templates (VPATs), can be made available on request through the reseller.

10. Data Protection and Security

Security, Data Protection and Certifications

Tricentis holds a wide variety of global certifications, providing evidence to support Public Sector customers in selecting Tricentis. Details of these certifications can be found at the following link: <https://security.tricentis.com/>

Tricentis strives to implement and continuously execute a proactive strategy for security and compliance. As a leader in test automation for cloud and enterprise applications, we are dedicated to providing peace of mind to our customers by applying policies and procedures designed to keep our data, platform, and products secure. Although no security program is 100% immune to compromise, we utilize security controls that exceed the standards for the environments in which we operate.

The service is delivered in accordance with recognised information security standards and is operated within a managed security framework. Data is protected through encryption in transit and at rest, role-based access controls, and secure authentication mechanisms. The service follows the principles of the UK GDPR and the Data Protection Act 2018.

Customer data remains under the Customer's control at all times and is used only for the purpose of delivering the service. Access to systems is restricted to authorised personnel and monitored through established security processes. Regular vulnerability scanning, security reviews and penetration testing are carried out to support the ongoing protection of the service. A Data Processing Agreement (DPA) is available on request through the reseller.

Information Security Management

The service is delivered in accordance with formal information security controls based on industry-recognised standards. Tricentis maintains an Information Security Management System (ISMS) certified to **ISO/IEC 27001**, covering applicable SaaS platforms, internal processes, and organisational controls. Security policies are reviewed at least annually and monitored through formal internal audit, risk assessment, and continuous improvement processes.

The platform includes security measures such as:

- Role-based access control (RBAC)
- Multi-factor authentication (where enabled)
- Encryption of data in transit and at rest
- Secure software development lifecycle controls
- Regular vulnerability scanning and penetration testing.
- Logging and monitoring for security-related events

Access to the platform is authenticated and authorised using secure identity management controls, and user permissions are configurable by the Customer.

Data Protection Compliance

The service is compliant with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. A Data Processing Agreement (DPA) is available and forms part of the contractual terms applicable to processing of personal data. The DPA is available and will be provided through XMA upon request.

Customer data remains under the full ownership and control of the Customer. The service processes data only for the purpose of providing the contracted service and does not use Customer data for analytics, profiling, marketing, or any secondary purpose.

Customers may request:

- Data access
- Data rectification
- Data deletion
- Data portability

in line with applicable data protection regulations and the terms of the DPA.

Data Storage and Location

Data is stored and processed in the region each customer selects: European Economic Area locations (Ireland with replication in Frankfurt), the United States (Ohio, Virginia, Oregon), or Australia (Sydney). For deployments hosted in the customer's private cloud or chosen data centre, all data remains in that customer-selected location.

Details of data hosting regions applicable to each service are available upon request.

Security Testing and Assurance

Security assurance activities include:

- Independent external penetration testing
- Application vulnerability scanning
- Secure development lifecycle reviews
- Incident response exercises and risk assessments

Penetration testing is performed at least annually by qualified third-party providers. Identified vulnerabilities are managed through a structured triage and remediation process.

Customers are responsible for testing integrations or configurations within their own environments, including firewall settings, local policies, and connected applications.

Access, Audit and Logging

Administrative access is restricted to authorised personnel and based on the principle of least privilege. Changes to system configuration and security-sensitive activities are logged and monitored.

Audit data may be made available to Customers upon request for compliance or assurance purposes. Any audit engagement by the Customer or a third party must be coordinated through XMA and carried out in accordance with the terms in the underpinning agreement.

Incident Management

Security incidents are managed through a documented incident response process aligned to ISO 27001 controls. In the event of a personal data breach affecting Customer data, Tricentis will notify XMA without undue delay in accordance with applicable legal and contractual requirements.

Certifications and Compliance

The following certifications and compliance frameworks apply to relevant Tricentis services:

Area	Status
ISO/IEC 27001 Information Security Certification	Maintained and in scope for service
SOC 2 Type II (where applicable)	Available for select services; in scope expansion planned
UK GDPR and Data Protection Act 2018 Compliance	Yes
Vulnerability Scanning and Penetration Testing	Performed routinely

Copies of certificates or assurance summaries can be provided to XMA for validation or to support buyer assurance requests.

Customer Responsibilities

Customers are responsible for managing:

- User access and permissions
- Local endpoint and corporate network security
- Secure handling of exported data
- Identity and authentication policies linked to their environment.
- Security of third-party systems integrated with the service.

Customers must notify XMA of any suspected misuse of credentials, security issues, or unauthorised access.

11. Backup and Disaster Recovery

The service includes automated backups as part of standard platform operations. Backups are managed by Tricentis and stored securely in accordance with the service's retention and security controls. Backup and disaster recovery processes are monitored and periodically tested to support service continuity. Recovery times may vary depending on the nature of the incident and the service tier. Custom or Customer-initiated backup configuration is not included as part of the standard service. Customers are responsible for maintaining copies of exported data where internal retention policies require local storage.

12. Pricing and Commercial Information

Pricing and Commercial Information

Pricing for the services is provided in a separate pricing schedule available through the reseller (XMA) submission. The service is offered on a subscription basis, with pricing aligned to the number of users, length of subscription term (minimum term 12 months), and service tier selected. Pricing is stated in pounds sterling (GBP) and excludes VAT.

Standard pricing covers access to the service, platform maintenance, product updates, and support as defined within this Service Definition. Optional services such as onboarding assistance, training, or advanced configuration activities may be available at additional cost and will be outlined separately where applicable.

Discounts may be available based on committed subscription volumes or multi-year terms. Any agreed discount will apply at the point of purchase and will be reflected in the final order submitted through the G-Cloud framework. Discounts are applied on a per-transaction basis and do not constitute a standing or guaranteed rate for future purchases.

Trial access, pilot licensing, or evaluation arrangements may be available upon request via XMA. Where applicable, these will be time-limited and provided subject to approval.

Payment terms follow those stated under the G-Cloud Call-Off Contract, and invoicing will be submitted through XMA as the prime supplier.

13. Ordering Information

This service can be ordered through the G-Cloud framework using the Digital Marketplace. The purchase will be made through XMA as the prime supplier. Once an order is confirmed, XMA will notify Tricentis to provision the service according to the agreed subscription and service scope. No negotiation or modification of terms is permitted as part of the ordering

process, and all purchases are subject to the applicable G-Cloud Call-Off Contract terms and published service pricing. Any optional services, if required, must be arranged separately through XMA and are outside the scope of the standard ordering process.

14. Supplier Information

Prime Supplier:

XMA Ltd (United Kingdom)

Subcontractor / SaaS Provider:

Tricentis GmbH

Leonard-Bernstein-Straße 10

1220 Vienna

Austria

Company Registration: FN 268343 a (Commercial Court of Vienna)

VAT ID: ATU 62091439

Website: <https://www.tricentis.com>