

G-Cloud 15

Service Definition Document

**TraxQM - Risk based Quality Management System for
Regulatory Compliance**

Codesplice Ltd

Lot 2 Cloud Software

1. Introduction	3
Company Overview	3
Value Proposition	3
What the Service Provides	4
Social Value	4
Overview of the G-Cloud Service	5
Associated Services	9
Information Assurance	9
Data Back-Up and Restoration	9
Business continuity statement/plan	10
Privacy by Design	11
3. Using the service	12
Ordering and Invoicing	12
Availability of Trial Service	12
On-Boarding, Off-Boarding, Service Migration, Scope etc.	12
Training	12
Implementation Plan	12
Service Management	12
Service Constraints	13
Service Levels	14
Outage and Maintenance Management	14
Financial Recompense Model for not Meeting Service Levels	15
4. Provision of the service	15
Customer Responsibilities	15
Technical Requirements and Client-Side Requirements	15
Outcomes/Deliverables	16
Development life cycle of the solution	17
After-sales Account Management	17
Termination Process	18
5. Our experience	18
Case Studies	18
Clients	20
Contact Details	20

1. Introduction

Company Overview

We are a UK-based software company delivering SaaS products that help regulated organisations accelerate compliance, strengthen quality management, and meet industry standards with confidence. Our products, FMVerify, Trax2D, TraxCM, and TraxQM are purpose-built for pharmaceutical, life sciences, and ISO-regulated sectors, providing rapid implementation and immediate operational value.

Developed using deep in-house industry expertise and guided by leading regulatory specialists, our applications embed best practices, ICH guidelines, and real-world compliance intelligence. This ensures customers benefit from workflows and controls that are not only efficient but aligned with the expectations of regulators.

Our solutions streamline critical processes, reduce the burden of regulatory affairs, and give teams the tools to manage risk, documentation, quality events, and oversight with ease. Trusted by major wholesalers and manufacturers, including those working with CMOs, our platforms support organisations looking to modernise their compliance operations, unify data flows through integration with existing applications, and achieve audit readiness at all times.

With UKAS-accredited ISO 9001 and ISO 27001 certifications, we deliver software engineered to meet the security and quality demands of regulated industries. Our risk-based quality management system, endorsed by former senior MHRA inspectors, reinforces our commitment to compliance excellence.

Supported by a leadership team with extensive experience in technology, business management, and consulting, we combine modern engineering with high-touch service delivery, helping customers adopt smarter, faster, and more robust compliance practices.

Value Proposition

- Centralised content allows fast access, full traceability, and controlled visibility for every user.
- Embedded process-level risk assessment
- The application is fully web-based with a companion mobile app, ensuring secure and convenient access anywhere.
- A unified, consistent module design dramatically reduces training time.
- Designed to guide users into compliant, regulation-aligned workflows.
- Collaboration tools that keep everyone aligned, focused, and accountable
- As a GAMP 5 Category 3 application, users avoid costly validation exercises, with full validation reports supplied by us

Inspection authorities across the pharmaceutical and life sciences sectors continue to highlight recurring quality management deficiencies, often stemming from paper-based or hybrid QMS models that lack a risk-based approach.

TraxQM transforms quality management with a data-centric platform that aligns with ALCOA+ principles, ensuring compliance while simplifying processes.

It proactively addresses inspection gaps like realistic risk assessments, clearly defined severity, detailed controls, and robust Root Cause Analysis, helping organisations reduce regulatory risks, improve operational efficiency, and maintain audit readiness with confidence.

What the Service Provides

TraxQM, developed by **Codesplice Ltd**, is a cloud-based **Quality Management System (QMS)** delivered as Software-as-a-Service (SaaS). It enables regulated organisations to manage quality and compliance processes in line with GxP, 21 CFR Part 11, EU GMP Annex 11 requirements and various ISO standards for electronic records and data security.

The service provides:

- **Comprehensive Quality Modules** — The application comprises the following modules: Document Manager, Events Manager, Risk Analysis Manager, Change Control Manager, Audit Manager, Training Manager, and Management and Planner modules. As a SaaS product, it's constantly evolving, and new modules are introduced to further QMS controls within the organisation.
- **Automate Supplier Validation** — TraxQM integrates with MHRA, GPhC, Companies House and EUDRA to automatically pull verification data and attach it to the supplier record. We offer weekly automated checks against the MHRA revoked and suspended list.
- **Secure Cloud Hosting** — Fully managed on **AWS** with **Azure Entra ID** authentication, offering new user setup or single sign-on with enhanced access control.
- **Integrated AI Assistance** — For document, risk, and KPI reviews aligned with the GxP and MHRA regulatory guidelines.
- **Automatic Versioning and Audit Trails** — ensuring complete traceability and compliance with **21 CFR Part 11** and **Annex 11**.
- **Continuous Data Protection** — including encryption, backup, and high availability through AWS infrastructure.

Social Value

As a SaaS provider, we are committed to creating measurable, long-term social value through the delivery and management of secure, sustainable, and inclusive cloud-based services.

Our approach aligns with the UK Government's Social Value Model (PPN 002) and supports national priorities to:

- Kickstart economic growth
- Make the UK a clean energy superpower
- Break down barriers to opportunity
- Build an NHS fit for the future

We embed social value throughout our operations, delivery model, and supply chain, ensuring that every engagement contributes positively to people, the economy, and the environment.

Kickstarting Economic Growth

We support organisations transitioning from paper-based to digital compliance processes through our SaaS QMS platform to reduce administrative time and cost.

Measure	Target/Commitment
Adopt digital quality management tools	≥ 100+ new organisation

Making the Country a Clean Energy Superpower

Our designs replace manual, paper-driven QMS activities with digital workflows.

Measure	Target/Commitment
Document statistics (paper vs digital)	50% reduction in paper-based processes within 6-12 of system adoption

Breaking Down Barriers to Opportunity

Offer practical e-learning modules on compliance, document control, and risk management.

Measure	Target/Commitment
Post-training feedback survey	85% satisfaction from training participants

Building an NHS Fit for the Future

Our SaaS solutions enable improved efficiency and reduce administrative burden.

Measure	Target/Commitment
Digital transformation impact	15% reduction in administration processing time for clients

Monitoring and Reporting

We will monitor progress against these commitments through quarterly reporting and annual social value reviews, aligned to CCS reporting frameworks. Independent audits, customer feedback, and performance data will be used to validate outcomes and inform continuous improvement.

Overview of the G-Cloud Service

TraxQM, provided by Codesplice Ltd, addresses growing demands for regulatory compliance, digital transparency, and operational efficiency through a secure cloud-based Quality Management System available via the G-Cloud framework. It allows organisations to centralise and control their quality operations, supporting compliance with GxP, ISO 9001, ISO 27001, EU GMP Annex 11 and 21 CFR Part 11.

Delivered entirely as Software-as-a-Service (SaaS) GAMP 5 – Category 3 product, TraxQM removes the need for on-premises infrastructure and intensive in-house validation to allow smoother onboarding. It provides:

- **Centralised oversight** of Documents, Risks, Quality Events, Change Control, Training, Management Reviews, Supplier/Customer validations, Audits, Asset tracking and more.
- **Automated workflows** that improve consistency and reduce administrative effort.
- **Built-in security and traceability**, including validated audit trails and e-signatures.
- **Interoperability**, with REST APIs and Entra ID single sign-on.
- **Continuous improvement**, with updates and security patches applied by Codesplice Ltd.

Hosted on AWS across multiple data centres and utilising Azure Entra ID for authentication, the service combines resilience with data protection and privacy by design.

Primary Modules

Risk Manager:

- Requirements of GxP, ISO Standards – Establish processes, requirements, failure modes and effects and controls with severity, occurrence, and detection scores.
- Quality Events – Align multiple failure effects, each with multiple causes to a failure mode.
- Integrated RA table – Access RA table from within a Deviation, CAPA or a Change Control to check for considered Failure Modes, effects, and Root Causes.
- Record new controls – Move recommended controls to current controls at a slide of a toggle.
- AI assistance to review recommended controls.

Document Manager:

- Document life cycle management – creation, review, approval, implementation, use, withdrawal, destruction.
- Version control – Documents can be stored at draft, published, and archived stages. Provides versioning during the various stages of drafting and approval. Older published versions and draft versions can be downloaded. Published documents can be archived and can only be deleted after 5 years of publication. Status change can be invoked to place the documents in a draft or published state.
- User defined Tags – This functionality is provided to add additional information to documents and files so that they can be easy to categorise and find. Tagging removes the need to duplicate files in different folders. Tags can be given names and can be colour coordinated.
- CFR 21 Part 11 compliant digital signature-based approvals – No need to print and wet ink the documents. Digital signatures contribute to data integrity and conform to industry standards.
- DocuSign integration – Electronic signature functionality for documents that need to be sent to external parties for signatures.
- Built-in file viewer – Allows viewing of PDF, word, excel and PPT documents stored in the TraxQM eco-system.
- Edit Office files via locally install Office with auto-sync – Edit and save documents from within TraxQM. Documents can be created from templates stored in the document manager.
- Co-authoring support – Invite your colleagues to review the document before publication. Recipients can be invited to approve or reject document once in their final state.

- View Documents – Invite team members to view published documents with option to accept or reject.
- Comments box – A collaboration tool for communicating with colleagues about documents being created, reviewed, and published. Comments can be searched by contributor.
- AI assistance for document health check.

Event Manager:

- Identification – Log a Deviation, CAPA or Compliant with automated log number generation. A non-conformance can be classified as an Incident, which can be recorded and closed out and with the provision to record and track for trend analysis.
- Evaluation – A failure mode which is not an incident is evaluated for impact and risk. Record detailed information of the issue and associated evidence, including comments and attachments. Use tags to record specific details e.g., GTIN or batch number for trend analysis. Impact at the departmental level can be assessed and recorded, while a severity, occurrence and detection score will determine an escalation route of “No Action”, “Correction” or “CAPA”
- Investigation – With an unknown cause, instigate an investigation process to determine the areas of the QMS which fall short of meeting requirements, leading to the quality event.
- Analysis – Use 5-ways to determine potential causes and the Root Cause of the Event. Instigate a committee review to contribute to the proposed Root Cause. View the risk table to ensure risks and Root Cause are captured.
- Action Plan – Record a procedure for document changes, process changes, procedure or systems change, training, sampling and any monitors or controls required.
- Implementation – Raise tasks to implement the action plan. Attach evidence, including comments and attachments of completed tasks.
- Validation – Raise tasks to validate that the actions have been completed and check for the effectiveness of the results. Attach evidence.
- Review – Determine the effectiveness of risk evaluation by reviewing recalculated RPN numbers.

Change Control Manager:

- Identification – Describe the desired change and the reason for the change. Record any urgent changes made.
- Evaluation – Consider impact and associated risks for the proposed change. Consider existing severity, occurrence and detection and predicted severity, occurrence, and detection with new controls. The initiator or a committee can review the impact and risks to classify the change. View the risk table to ensure risks and Root Cause are captured.
- Action Plan – Describe directions for implementing and documenting measures, cross referencing affected documents that require revision, training to be conducted, pre-change activities and critical tasks. Raise verification tasks to gain confidence in proposed direction.
- Implementation – Raise tasks in order of priority with option to re-schedule. Attach evidence of completed tasks. Show status of tasks.
- Validation – Raise tasks to validate that the actions have been completely correctly and check for the effectiveness of the results. Attach evidence.
- Review – Determine effectiveness of risk evaluation by reviewing recalculated RPN numbers, with an option to raise a further CAPA.

Training Manager:

- Ready to use training courses library.
- Gamification and certification.
- Build your work course with built-in editor.
- Create multiple teams and learning paths.
- Support for SCORM, xAPI and cmi5.
- Host live sessions, tests, and quizzes.
- Training reports (exportable excel sheets).

Audit Manager:

- Audit Program – Set up audit criteria and scope against specified time frames. Commit processes, clauses, or departments to the specific programs.
- Audit Plan – Create a checklist by drawing out the requirements of the standard from the risk table. Define sources for evidence including previous audits, CAPAs, SOP, training records etc. Determine methods for audit.
- Conduct Audit – Review and record evidence and determine conformance. Record a conformance, non-conformance, or a comment. Raise tasks for a non-conformance.
- Audit Report – Summarise audit positives, negatives, recommendations, future actions with related dates and any CAPA reference.

Returns and Recall Manager:

- Management of recall.
- Testing and recording of recall process.
- Management of returns.
- Recording and reporting Adverse Reactions.
- Recording and dealing with Falsified Medicines.

Management Module:

- Management reviews.
- Organogram
- Hardware and software Asset tracking and maintenance.
- Organisation context, interested parties, business objective, SWOT analysis.

All G-Cloud customers will receive the following services.

- Onboarding Support – Guidance and setup assistance to ensure smooth deployment and configuration of TraxQM.
- Data Migration – Support for importing existing quality records and documents into the TraxQM environment.
- User Training – Comprehensive end-user and administrator training sessions during implementation. Training is delivered remotely via Teams or on-site by our implementation team, ensuring a smooth transition from existing systems to the TraxQM environment.
- DocuSign Enterprise eSignatures – Fully integrated 21 CFR Part 11-compliant electronic signatures for approval workflows.
- Access to Over 1,000 Pre-Built Training Courses – Delivered via the integrated Training Module.

- Unlimited Secure Storage – All customer data is securely hosted within AWS (EU region) under a fair usage policy, ensuring high availability and scalability.

Associated Services

The following elements fall outside the scope of the standard costed model:

- Custom Development – Any customised development work needed to integrate the service with the client's existing applications or systems will be reviewed, and the necessary estimates will be provided.
- Additional DocuSign E-Signatures – Any usage beyond the agreed number of e-signatures included in the client contract will incur an additional charge.

These items will be scoped and costed separately as per our pricing document to ensure transparency and flexibility in meeting the client's specific requirements.

Information Assurance

Codesplice Ltd is a UKAS ISO 9001:2015 certified company, committed to maintaining the highest standards of information security, data protection, and operational integrity in line with UK Government and international best practices:

- TraxQM supports compliance with 21 CFR Part 11, EU GMP Annex 11, and GxP data integrity principles.
- The system design incorporates "privacy by design and default" as required under UK GDPR.
- Codesplice Ltd maintains documented Information Security, Access Control, Incident Management, and Business Continuity policies reviewed annually.
- Security patching and vulnerability management follow a defined schedule with continuous monitoring of system health and performance.
- As standard, the Backup and disaster recovery measures are implemented to achieve a Recovery Point Objective (RPO) of 24 hours and a Recovery Time Objective (RTO) of 4 hours.
- Data retention, deletion, and disposal are carried out in accordance with GDPR principles and customer agreements.

Data Back-Up and Restoration

Codesplice Ltd implements robust data backup and restoration processes for TraxQM to ensure business continuity, data integrity, and protection against accidental loss or system failure. All backup operations are automated, monitored, and reviewed as part of the company's information security and service management processes.

Backup Strategy:

- All core TraxQM data, databases, and configurations are hosted within AWS (EU region) and protected using the AWS Backup service.
- Backups are performed automatically with point-in-time recovery options.
- Document files stored in the integrated Microsoft SharePoint environment are backed up using Microsoft Backup (Microsoft 365 Backup Service) in accordance with GxP retention and redundancy policies.

- Backups are encrypted both in transit and at rest using AES-256 encryption and stored within separate AWS & Azure availability zones for redundancy.

Restoration and Recovery:

- Backup restoration can be initiated by authorised Codesplice Ltd personnel upon customer request.
- Recovery testing is conducted quarterly to ensure reliability and data integrity.
- The standard Recovery Point Objective (RPO) is 24 hours, and the Recovery Time Objective (RTO) is 4 hours for standard system components.
- Restoration requests can be raised via the TraxQM support desk under the service's incident management process.

Review and Governance:

- Backup configurations and policies are reviewed quarterly as part of the company's ISO 27001-aligned information security management system (ISMS).
- All backup and recovery logs are retained and auditable.
- Any client-specific SLA, data retention or backup requirements can be agreed and documented in the Order Form prior to service commencement.

These combined measures ensure that TraxQM maintains continuous data availability, protection, and recoverability in line with good industry practice and public sector expectations.

Business continuity statement/plan

The Codesplice Ltd Business Continuity Plan (BCP) applies to all systems, processes, and personnel responsible for delivering and operating the TraxQM cloud service. Its aim is to ensure the continuation of essential business operations and safeguard customer data in the event of service disruption, system failure, or external incident. The following is a summary intended as an overview; a more detailed plan can be provided to the buyer on request. The plan covers the following business areas that are essential to service delivery:

- **Application Hosting and Infrastructure Management** – availability, uptime, and performance of AWS & Azure hosted environments. The service runs over an Active-Active load-balancing architecture, allowing it to remain available even in the event of an outage in any given data centre.
- **User Authentication and Access Control** – managed through Azure Entra ID for secure identity management and continuity of access.
- **Data Storage and Backup Operations** – ensuring the integrity and recoverability of all customer data.
- **Customer Support and Communication** – maintaining client communication channels during incidents through alternative routes.
- **Development and Maintenance** – ensuring controlled release management and service restoration capability.

Critical Functions:

- TraxQM platform availability and access.
- Customer data protection and backup restoration.
- Authentication and authorisation continuity.
- Customer communication and support response.

Dependencies and Interrelationships:

Critical dependencies include AWS (EU region) for application hosting, Microsoft Azure Entra ID for user authentication, Microsoft SharePoint for document storage, and Docusign for eSignature. Each dependency is managed under formal vendor agreements with continuous service monitoring and escalation procedures in place.

Acceptable Downtime:

- **Critical System Functions:** Recovery Time Objective (RTO) – 4 hours
- **Data Recovery:** Recovery Point Objective (RPO) – 24 hours

Above SLA is part of the standard objectives that are reviewed annually and verified through recovery testing. Custom SLA requirement with shorter RTO and RPO can be arranged as per the client's requirement.

Privacy by Design

Codesplice Ltd integrates Privacy by Design and by Default principles throughout the development, deployment, and operation of the TraxQM. The system is designed to comply with the UK GDPR, the Data Protection Act 2018, and relevant EU data protection laws.

Privacy and data protection are integrated from the earliest stages of TraxQM's design process. Every new feature or enhancement undergoes a Data Protection Impact Assessment (DPIA) to ensure that data minimisation, lawful processing, and user consent requirements are met before implementation. Key features of our processes are as follows:

- Only essential personal data is collected and processed, limited to user identification, authentication, and audit trail purposes.
- Role-Based Access Control (RBAC) and Azure Entra ID authentication ensure that users only access information necessary for their role.
- All data is encrypted in transit using TLS 1.2 and at rest using AES-256.
- Audit logs record all user activity, including modification events.
- Backups are encrypted and stored securely in multiple datacentres.
- Regular penetration testing and vulnerability assessments are conducted to identify and mitigate potential risks.
- Third-party processors are reviewed annually to ensure ongoing compliance with GDPR and ISO 27001 standards.

Through these measures, TraxQM ensures that privacy is not an afterthought, but a core design principle that safeguards user data while supporting compliance, transparency, and trust.

3. Using the service

Ordering and Invoicing

The user can request a demo of the service and subscription cost by sending an email to info@codesplice.com. Once the client confirms their intent to onboard, the supplier will issue a statement of work (SOW) and a software maintenance agreement. Subscription is charged monthly. The user will need to inform the supplier of the service of their intended onboarding date.

Availability of Trial Service

The service provider offers a trial version of the service; however, certain functionalities involving integration with external systems are not included in the trial.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

Pre-onboarding templates for easy onboarding, lift and shift of documents and unlimited training and validation is included as part onboarding.

After deployment is completed, a trained facilitator will organize training sessions tailored to users' requirements and schedules. A comprehensive user guide will be provided as part of the deployment.

The contract allows either party to terminate after the first year, provided three months' notice is given before the one-year anniversary of deployment. A plan would be agreed with the user to export, expunge or delete client data.

The service provider can provide additional services to help migrate away to a new service provider.

Training

A qualified trainer provides instructor-led training, while users can additionally undertake self-guided training using the supplied user guide.

Implementation Plan

An implementation plan can be provided to the buyer on request.

Service Management

Our service management approach delivers a secure, resilient, and customer-focused SaaS experience. By combining industry best practices with proactive governance and innovation, we ensure long-term value, compliance, and operational excellence for both private and public sector clients.

Governance and Compliance

Our service management model is built on ITIL and ISO 20000 principles, ensuring consistency, accountability, and transparency. We maintain compliance with international standards and sector-specific regulations, including Cyber Essential Plus, GDPR, ISO 27001, and SOC 2, while tailoring our approach to public sector governance requirements. Regular audits, SLA reviews, and risk assessments underpin our commitment to regulatory adherence and service integrity.

Service Delivery and Support

We provide a 24/7 service desk with tiered support (L1–L3) to ensure rapid incident resolution and minimal service disruption. Structured processes for incident, problem, and change management drive operational efficiency and prevent recurrence of issues. Service requests are managed through a defined workflow, with clear escalation paths and regular service performance reporting.

Availability and Continuity

The SaaS platform is designed for resilience, leveraging high-availability architectures and multi-zone redundancy. Our business continuity and disaster recovery (BC/DR) plans are tested regularly, ensuring defined RTO/RPO objectives are met. Automated backups, failover mechanisms, and capacity management guarantee consistent service availability to meet client SLAs.

Security and Data Protection

Security is embedded across every layer of our service. We enforce role-based access control, encryption of data in transit and at rest, and continuous security monitoring. Regular vulnerability assessments, patch management, and incident response processes safeguard client data. For public sector clients, data residency and sovereignty requirements are strictly adhered to.

Performance and Monitoring

Comprehensive monitoring tools track performance across infrastructure, application, and service layers. Automated alerting ensures rapid detection of anomalies, while trend and capacity analyses enable proactive scaling. Regular performance reviews drive optimization and ensure the platform consistently exceeds agreed KPIs.

Customer Engagement and Communication

Each client is supported by a dedicated Service Delivery Manager who oversees day-to-day service performance and strategic alignment. We maintain open communication through regular service reviews, maintenance notifications, and incident updates. Feedback loops and satisfaction surveys drive our continuous improvement process.

Service Improvement and Innovation

Through our Continuous Service Improvement (CSI) framework, we analyse performance metrics and customer feedback to identify opportunities for enhancement. Root cause analysis, structured change management, and innovation roadmaps ensure the service evolves in alignment with client needs and technological advancements.

Vendor and Third-Party Management

We manage all cloud infrastructure and integrated third-party services under strict performance and security controls. Vendor SLAs are regularly reviewed to ensure compliance and seamless integration across the service delivery chain.

Service Constraints

Performance: Access to the modules is dependent on internet connectivity. The application and its modules are generally accessible without delay, except during occasional service disruptions originating from the underlying Cloud providers, AWS or Microsoft.

Availability: The service remains available on demand, with the exception of planned maintenance windows required for applying bug fixes or performing version upgrades with an intended 99.9% uptime.

Support hours: Support is available during working hours to address knowledge transfer, training or system issues. Under the Service Level Agreement, the provider will respond within five hours to advise on the anticipated duration required to resolve the issue.

Maintenance Windows: There are no predefined maintenance windows; however, any required maintenance will be scheduled during periods of minimal user activity, and all service users will be notified well in advance.

Level of Customisation Permitted: The service is a GAMP 5 Category 3 off-the-shelf application with no customisation. It offers sufficient flexibility for buyers to tailor configurations to their needs, and the service provider considers feature requests that could benefit the broader user base.

Schedule of Depreciation of Functionality/Features: The service is not expected to retire any features.

Service Levels

Service Level Actions refer to the remedial actions that the Supplier can implement to address and resolve issues affecting the application, where such issues fall within the Supplier's direct control. This excludes any incidents or dependencies managed by associated or third-party service providers outside the Supplier's control.

- Priority 1 - Critical
 - Complete loss of service / Major impact on essentials operations
 - Resolution Target - 4 Hours
 - Availability 24/7
- Priority 2 - High
 - Degraded performance / key function unavailable
 - Resolution Target - 8 hours
 - Availability - Business hours
- Priority 3 - Medium
 - Minor impact / workaround available
 - Resolution Target - 2 business days
 - Availability - Business hours
- Priority 4 - Low
 - Minor Low / General query / cosmetic issue
 - Resolution Target - 5 business days
 - Availability - Business hours

Outage and Maintenance Management

Maintenance Planning: A comprehensive maintenance plan is in place to outline scheduled times for updates and upgrades. The plan will detail the scope of maintenance, including the affected modules, the frequency of maintenance activities, and an assessment of potential impact on users.

Outage Management: Incidents are proactively monitored using a range of tools to detect outages and performance degradation. They are classified and prioritized by severity and business impact, with a CAPA process initiated to identify the root cause and resolution procedures implemented to restore service promptly and safely.

Communication: Users are notified in advance of planned maintenance, kept informed in real time during outages or issues, and provided with post-event reports summarizing the impact once service is restored.

Roles and Responsibilities: The service provider maintains a record of personnel responsible for performing updates and fixes, managing unplanned outages, and communicating with users and stakeholders.

Documentation and Tracking: Records are maintained for all scheduled activities, along with incident logs documenting outages, their causes, and resolutions. Actual uptime and response times are tracked against the agreed service levels.

Risk Management: An impact mitigation strategy is implemented, covering backup systems, failover, and redundancy, while change controls are applied on a risk-based basis to ensure maintenance or updates do not cause outages.

Review and Continuous Improvement: Outages and maintenance events are reviewed to improve scheduling, monitoring, and response procedures, with user feedback incorporated into the enhancements.

Financial Recompense Model for not Meeting Service Levels

The SLA provides 99.7% uptime. If the monthly uptime falls below the stated level the client may be eligible for the following service credit.

Monthly Uptime	Service Credit
<99.7%	50% of monthly fee
<99.5%	75% of monthly fee

The client must submit a claim to customer support at Codesplice which should include:

- Description of the incident
- Details of the duration of the down time
- Number of users affected
- Details of the actions taken during the downtime

4. Provision of the service

Customer Responsibilities

The customer is required to execute the SOW and Software Maintenance Agreement, which includes a non-disclosure clause, and make timely payment against issued invoices.

Technical Requirements and Client-Side Requirements

To ensure the effective deployment and operation of the service, the client is required to maintain certain technical and organisational prerequisites. These requirements support compatibility, system performance, and a successful implementation outcome.

- **Connectivity and IT Configuration**

The client must ensure adequate internet connectivity and manage their own IT environment, including Microsoft configurations, to support access to and use of the service.

- **Browser Requirements**

The service is supported on Google Chrome (version 140 or later) and Microsoft Edge (version 140 or later). The client is responsible for ensuring that users access the service through one of these approved browsers.

- **Single Sign-On (SSO)**

To enable single sign-on functionality, the client must have a Microsoft 365 email environment correctly configured and operational prior to implementation.

- **Implementation Preparation**

As part of the onboarding process, the client will be required to complete predefined implementation templates provided by the service provider. This activity will assist the client in determining how various components of their Quality Management System (QMS) will be structured and organised within the eQMS.

Outcomes/Deliverables

Deliverables

- Access to the SaaS application and all licensed modules.
- User accounts and role-based access control setup.
- Onboarding and training materials, including a user guide.
- Configuration and setup aligned to client's requirements (within permitted flexibility).
- Service documentation, including SLA details and support contacts.
- Regular updates, patches, and version upgrades as part of the subscription.

Outputs

- Real-time access to data and application features.
- Automated workflows, reporting, or analytics generated by the application.
- Notifications, alerts and dashboards.
- Monitoring and support outputs, such as incident logs and resolution tracking.
- Performance metrics tracked against agreed SLAs (e.g., uptime, response time).

Outcomes

- Improved operational efficiency through automation and streamlined processes.
- Reduced IT overhead due to cloud hosting and SaaS management.
- Enhanced decision-making through real-time analytics and reporting.
- Secure, reliable, and compliant access to the application.
- Flexibility to scale usage according to business needs.
- Reduced risk of downtime due to proactive monitoring and maintenance.

Development life cycle of the solution

TraxQM is developed using an Agile Kanban methodology, with all work tracked in Atlassian JIRA using a continuous flow model. The development process follows the stages below:

- **Identify needs:** Requirements gathered from clients, internal stakeholders and regulatory updates.
 - **Plan:** Work items captured as user stories and prioritised on the Kanban board.
 - **Design:** User journeys and interface mock-ups created in Figma. Clients review and approve prototypes before development begins, ensuring clarity of logic and allowing refinement of user stories.
 - **Build:**
 - Code is maintained in Bitbucket using separate branches for development, UAT and production.
 - All initial development is completed as per JIRA tickets and merged into the dev branch, with peer review and secure coding controls using linters and code quality review via Codacy.
 - Unit & Functional tests are performed on the dev branch before promotion.
 - **Test:**
 - When the code is deployed to the dev environment, E2E testing is performed using Ghost Inspector.
 - Runtime errors are captured using Sentry and AWS CloudWatch. And a further patch is deployed if required to fix the issues.
 - Once development passes internal checks and milestone criteria, the code is deployed to the UAT environment.
 - Further Security tests and end-to-end (E2E) testing are performed in UAT. And release documents are generated.
 - A demonstration is delivered to the project's steering group for final approval before production release.
 - **Deploy:** Our products are deployed on AWS, and the CI/CD process is fully automated. The environment is completely isolated with separate AWS accounts for development, UAT, and production. The automated, multi-account approach reduces deployment risk, eliminates manual error, and ensures consistent release processes.
- Upon approval, the code is merged into the respective branch in BitBucket, automatically triggering deployment to the corresponding AWS account through AWS CodePipeline.
- **Maintain:** Continuous monitoring is performed via logging tools such as Sentry, AWS CloudWatch & Snyk; incident response, optimisation, and minor enhancements are carried out routinely.
- Client and user feedback are recorded in JIRA and are fed back into the Kanban cycle for future improvements.

After-sales Account Management

We build and maintain customer relationships through structured onboarding, personalised account management, and responsive support. We proactively communicate updates, act on customer feedback, and provide value-added insights and resources to help clients achieve their goals, fostering long-term trust and partnership.

Termination Process

The Initial Term of this Call-Off Contract shall be four (4) years. The Customer may extend the Call-Off Contract for one or more periods up to a maximum of twenty-four (24) months in total. Either Party may terminate this Call-Off Contract by giving thirty (30) days' written notice

5. Our experience

Case Studies

Risk Based electronic quality management system

Like many organisations, Sigma Pharmaceuticals was using a hybrid quality management system, relying on paper documents and Excel sheets to represent their quality processes and record information on risks, training, customers, suppliers, and assets. Following a requirement from the National Competent Authorities to incorporate process-level risk assessments, Sigma decided to adopt TraxQM given the platform's functionalities are designed to reinforce the principles and expectations set out in:

ISO 9001:2015 (Quality Management System)

- Risk-Based Thinking: The system embeds structured, process-level risk assessments (FMEA), aligning with ISO 9001 requirements to integrate risk into organisational planning and operations.
- Documented Information Control: Version control, audit trails, user permissions, and digital workflows support robust management of documented information.
- Corrective and Preventive Action (CAPA): The system formalises incident management and CAPA processes, ensuring effective root-cause analysis and sustained corrective actions, consistent with ISO 9001 clauses.
- Performance Evaluation: Real-time dashboards and trend analytics facilitate the monitoring, measurement, and analysis of QMS performance.

Good Distribution Practice (GDP)

- Data Integrity: TraxQM supports GDP principles (ALCOA+), ensuring data is attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available.
- Deviations, Complaints, and Recalls: Configurable workflows allow Sigma to manage GDP-related quality events in a compliant and traceable manner.
- Training Compliance: Integrated training management ensures personnel have documented up-to-date training, aligned with GDP responsibilities.
- Supplier and Customer Oversight: Record management and audit tools support the qualification and ongoing monitoring of GDP partners.

MHRA Expectations

- Governance and Oversight: Real-time reporting and audit trails strengthen the organisation's ability to demonstrate effective QMS oversight to regulatory inspectors.
- Electronic Records and Signatures: Digital controls, permissions, timestamps, and traceability support compliance with MHRA expectations for electronic quality systems.
- Quality Risk Management: The platform's embedded QRM approach aligns with MHRA guidance encouraging systematic and documented risk evaluation.
- Inspection Readiness: Consolidated data, intuitive traceability, and process standardisation ensure Sigma can rapidly retrieve evidence during MHRA inspections.

ISO accreditation

Neupharm, an EU-based company, sought ISO 9001 certification and wished to adopt a fully digitised quality management system rather than a traditional paper-based approach.

They wanted the application to provide the following capabilities.

- Provides intuitive user guidance, contextual help, and prompts to ensure users enter accurate and complete information.
- The system supports controlled document creation, approval workflows, version control, access permissions, and audit trails.
- The system allows clear creation, visualisation, and maintenance of process flows.
- The platform supports formal risk assessments, scoring, mitigation actions, and ongoing monitoring.
- The system provides tools to schedule internal audits, assign auditors, track progress, and record findings.
- Supports recording minutes, decisions, action items, and outputs from management reviews.
- The solution allows creation, investigation, tracking, and closure of non-conformances and corrective actions.
- The system provides tools to create and track training, assess competency, maintain a skills matrix, and assign training based on roles or risk.
- The platform includes registers for customer and supplier information with the ability to evaluate, categorise, and monitor performance.

Having already implemented TraxQM to achieve GDP compliance, Neupharm is now using the application to support its progression towards ISO 9001 accreditation.

Benefits

- Ensures ongoing identification and management of stakeholder needs, supporting ISO 9001 requirements for understanding interested parties.
- Aligns quality objectives with the expectations of interested parties, improving strategic direction.
- Strengthens risk-based thinking by enabling measurable evaluation of controls and their effectiveness using performance indicators.
- Provides clear understanding of the organisation's internal and external context, supporting strategic planning.
- Facilitates structured assessment of strengths, weaknesses, opportunities, and threats to support risk-based planning and strategic decision-making.
- Improves control of external providers through systematic evaluation and monitoring, enhancing supplier performance and ensuring conformity of purchased products/services.
- Ensures competence and availability of required resources, strengthening workforce capability.
- Enhances continual improvement by verifying whether corrective and preventive actions are achieving desired results.
- Supports strategic alignment and continual improvement by maintaining and reviewing business and quality plans to ensure they remain effective and relevant.

Clients**Contact Details**

T: +44(0)333 444 3150

E: info@codesplice.com