FORTESIUM

Regulator Online

Service Definition Document

G-Cloud 14

May 2024

CYBER ESSENTIALS PLUS

Microsoft Partner Network

Crown Commercial Service

INSTITUTE OF REGULATION

nqa. ISO 9001

nqa. ISO 27001

Service Overview

Regulator Online is regulatory software provided by ex-regulators. Over the past 14 years Fortesium have built the only UK cloud software company providing commercial off-the-shelf solutions, designed exclusively for regulators.

Our ongoing mission is to empower our clients with the tools and expertise required to digitalise and automate their processes.

For us, a successful partnership sees our product save your organisation time, money and resources allowing you to concentrate on new challenges whilst Regulator Online takes care of the rest.

Trusted by over a million registrants.

We estimate that one in three of the UK's regulated professional use Fortesium software as a part of their registration, that's over one-million professionals along with tens of thousands more regulator team members, members of the public, other professionals, and institutions.

In healthcare alone, Fortesium software is used by over 45% of people regulated by the Professional Standards Authority (PSA) regulators, and three of the PSA's ten key regulators choose Fortesium.

Solutions delivered on time and on budget.

We are technology experts with a deep understanding of regulation. Our consultants have over 50 years of experience working with and for UK regulators. We take the time to understand your organisation and its requirements. We speak your business language, and we can add value to you business requirements.

Regulator Online – An all-in-one regulatory hub.

Developed over the last 6 years, Regulator Online is the realised dream that sparked the creation of Fortesium – an all-in-one regulatory hub to automate and streamline any regulatory procedure.

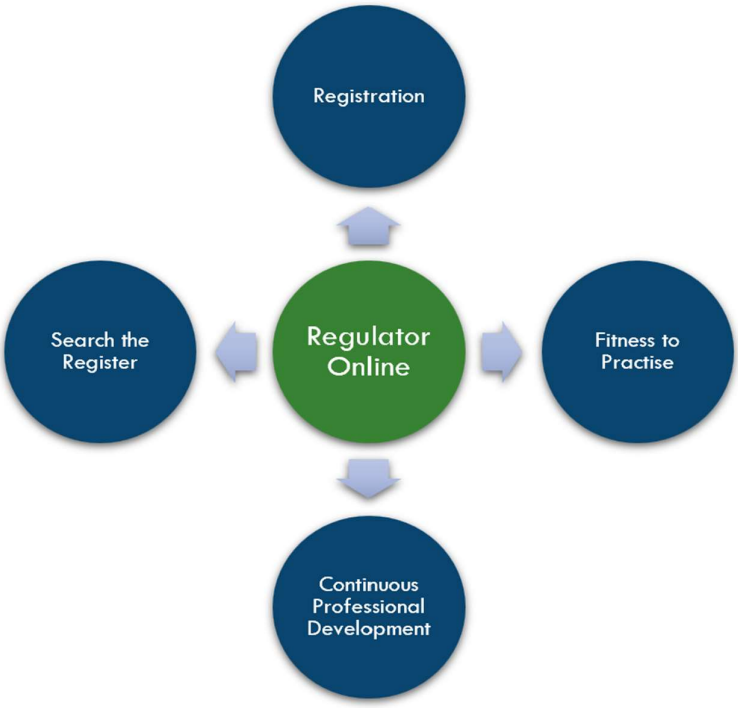
Designed using user-first methodology, Regulator Online's sleek and intuitive interface neatly compartmentalises your processes into key modules, each of which enable you to overview a full history of previous tasks and applications.

Streamline clunky processes, automate the mundane and drive faster outcomes with one innovative piece of software, freeing up resources to focus on exception or risk. Modules include:

- Registration
- Fitness to Practice (FtP)
- Search the Register (StR)
- Continuous Professional Development (CPD)

FORTESIUM

Regulator Online Modules



Company Values

Data Management, incident and business continuity arrangements

Fortesium solutions are hosted within Microsoft Azure to ensure their resilience and availability. Microsoft Azure services achieve service resilience through redundant architecture, data replication, and automated integrity checking. Redundant architecture involves deploying multiple instances of a service on geographically and physically separate hardware, providing increased fault-tolerance for Microsoft Azure services.

Each component of Regulator Online is hosted in Microsoft Azure which guarantees very high rates of uptime for all infrastructure components. Specific SLA examples are shown below for various Azure based services that are part of the Regulator Online infrastructure options.

- Monthly Uptime %= 100 * (Maximum Available Minutes-Downtime) / Maximum Available Minutes
- SQL Azure: 99.99% monthly uptime
- Virtual machines: 99.9% monthly uptime
- Azure Bot Service (Premium): 99.9% monthly uptime
- DDOS Protection Service: 99.99% monthly uptime
- Power BI Embedded: 99.9% monthly uptime
- Storage SLA: 99% monthly uptime

Microsoft Azure core compute services ran at 99.995% average uptime across the global cloud infrastructure from July 2018 to July 2019 (Source: https://azure.microsoft.com/en-gb/blog/advancing-microsoft-azure-reliability/)

Fortesium solutions are hosted within Microsoft Azure which ensures a high level of support for disaster recovery. Microsoft Azure supports multiple mechanisms for handling DR, for example:

- Active geo-replication
- Auto-failover groups
- Geo-restore
- Zone-redundant databases

If using zone redundant premium or business critical databases or pools, recovery is automated in the case of an outage.

Our deployments use Azure Container Apps which supports availability zones (multiple deployments across three physically separate groups of datacentres within each Azure region)

Back up

Data backups are provided by Microsoft Azures' SQL Server built in and fully automated backup mechanisms. These consist of full weekly backups, differential backups every 12-24 hours and transaction log backups ever 5-10 minutes (depending upon computational requirements and volume of database activity).

This means that data recovery can take place to anywhere in a 10-minute window, allowing for a fine-grained approach to recovery.

Long term backups can be held for up to 10 years, if required. These backups can then be restored as a new database.

With Regulator Online, clients can revert to any backup held over the supported period, in a matter of minutes and be confident that all data (including backups) is fully secured.

Fortesium's standard client database back-up retention PITR (Point in Time Restore) is 7 days, 24 hour back up frequency and 6 months of weekly backups retained (first week of every month). The above outlines our standard retention policy, however each client's needs are assessed on a case-by-case basis. We can revert to the most recent back up in the event of system failure during transaction processing. In most cases of failure during transaction processing, a failure message will automatically retry and be successful, without data loss occurring.

Onboarding Process / Approach to Implementation

At Fortesium, we take an agile approach to project management. An agile approach uses short cycles or sprints to customise our 'off-the-shelf' product. This means the project team produces frequent deliverables (2-3 week sprints as agreed) in the form of completed user stories. Each element that is customised or developed in a bespoke way can then be tested and any defect resolved as the project progresses. We prioritise quick delivery, adapting to change and collaboration rather than rigidly following a fixed plan. Having worked with regulators for 14 years on projects like this, we know that this approach works; it helps senior stakeholders see early results, allows us to adapt to unforeseen change, and ensures risk of project slippage is kept to an absolute minimum.

Using our experience of working in an agile way, and exclusively with regulators, we have developed our own 'Fortesium methodology'. This methodology combines an agile approach with what we know works well for regulators in terms of governance and reporting. The key stages of our methodology are outlined below with a short description:

- **Project Start Up**

  At this stage we define roles and responsibilities for both Fortesium and the client project team members. This includes an estimate of time commitment for each role to ensure the appropriate personnel can be selected. We agree and establish hosting arrangements, high level project timelines, discuss business constraints and any early risks. We also identify any third parties we need to engage with to deliver our solution, so we can pursue early engagement with key players. These early discussions can allow our Project Manager to draft a Project Inititation Document (PID) to be shared with the client team at the pre-discovery stage for review and amendment. Prior to this meeting our technical team will establish a test environment to be used throughout the project.

- **Pre-Discovery**

  At this stage we hold an initial face-to-face meeting with the client team once roles have been defined. We would typically come to your offices in person with our delivery team. This is an opportunity to outline our processes, discuss expectations on both sides, establish preferred communication methods for day-to-day delivery, give an overview of DevOps, provide DevOps access to team members, discuss the high-level project plan and key milestones and present a draft PID for review. Hosting arrangements will also be discussed and agreed.

- **Discovery**

  The discovery stage involves further face-to-face sessions where our team will travel to the client offices whenever possible. As an alternative, discovery sessions can also be facilitated via MS Teams to accommodate any home working practices. We

usually run these as full day sessions, but we can be adaptable to meet client needs. During the sessions we typically provide a short demo of ROL, discuss and agree a high-level communications plan, complete or review 'as-is' process diagrams and map 'to-be' processes. During the discovery process, there may be a number of these process mapping sessions, and in between sessions, our Business Analyst will create draft epics, features and user stories in DevOps for your input and review.

- **Configuration (including bespoke development and integrations)**

  Once we reach the stage of discovery where we have 3 weeks' worth of user stories completed and signed off by the client team, we can commence the first development / customisation sprint. During development work, any queries arising from the Configuration Consultants will be directed to the client team via MS Teams, or by email, to ensure any assumptions they hold are correct, and to prevent any need for future alterations which could cause delays. We find this real time 'back-and-forth' communication really helps build and develop team relationships and ensures the pace of work remains consistent with an agile approach.

- **Environment (MS Azure hosting arrangements and Pre-Production environments established)**

  This is a relatively short but very important phase during which our technical team establish pre-production and production environments in MS Azure. Hosting arrangements can be discussed and agreed during the pre-discovery stage.

- **System Testing**

  Each new element of our product that is developed or configured goes through rounds of testing starting with the Configuration Consultants unit testing before deployment. This is followed on a sprint level by sprint testing undertaken by our Test Analysts. Each iteration is tested at the sprint level during configuration, followed by a full, end-to-end regression test at the close of this stage of the project.

- **Export, Transform and Load (ETL) / Data Migration**

  Data is migrated using our ETL approach, first as a test migration to pre-production to ensure all parties are content with the approach and the outcome, followed by a complete migration as specified to the production environment. The stage of the project that ETL is viable may vary depending on a range of factors. This will be determined with the client during the discovery phase.

- **Training**

  Training is provided to admin users through a variety of mediums such as online training sessions, training videos, and training manuals. The training program can be flexed and adapted to the needs of the client, however, given the intuitive nature of our products, the time and resource required to deliver training is usually minimal. Typically, an admin user can become familiar with our products after just a few hours reviewing our training videos at their own pace along with the ability to apply their new knowledge in the test environment.

- **User Acceptance Testing (UAT)**

  Once our team have tested all elements of the client solution from end-to-end and any defects have been identified, resolved, and retested, we provide the client team

time to fully test the solution from end-to-end in pre-production. Any issues identified at this stage can be logged as defects or discussed as changes to be resolved prior to go-live.

- **Deployment / Go-Live**

  Once UAT has been signed off by the client, our technical team can deploy to the production environment in time for the go-live date outlined in the project plan. We will communicate with client colleagues regularly during this time to ensure you are aware when and how each element will happen, and to support with any non-functional requirements or communications necessary prior to this happening. Contact can be anything from daily-contact to hourly-contact, depending on the preferences and requirements of the client.

- **Hypercare**

  After go-live we will provide a period of intensive support that we will refer to as Hypercare. During Hypercare, the Fortesium core development team will remain available to the client to ensure any teething problems are resolved quickly following the launch. The period of Hypercare required by the client can be discussed and agreed during the pre-discovery stage.

- **Support and Maintenance**

  During the transition from Hypercare to Support and Maintenance the Project Manager will undertake a formal handover with the Customer Success Manager. During this period, regular contract management meetings will be established, users will be familiarised with all the channels by which support tickets can be raised, and the project delivery team will remain available on an ad hoc basis to provide any support required to ensure excellent levels of service for the duration of the contract.

Offboarding / Exit Approach

In line with our ISO 27001 (Information Security Management Standard) and ISO 9001 (Quality Management Standard) accreditations, we have well-established, best-practice exit and decommissioning procedures in place.

We can deliver an exit plan at contract commencement or when exit procedures are initiated depending on client preference. As an outline, the exit plan will:

- Define the target state and specify deliverables for Fortesium.
- Be a managed project (once we have received the timeframes); all key tasks and milestones will be mapped onto a project plan that can be shared and agreed with all stakeholders. A Fortesium Project Manager familiar with the client would manage the exit strategy as a project.
- Include a migration plan – in much the same way we would plan for data migration during the implementation phase, we would plan to extract data and transform it into the format preferred by the client or as specified by a new supplier. This will be a collaborative exercise during which we will engage with the new supplier, third parties where there are existing integrations, client team and if necessary, the hosting provider.

- Risk assessment – each data asset will be risk assessed in relation to any migration activity and appropriate mitigation measures put in place to satisfy all parties that any risks are well managed.
- Scenario based exit contingency plans – our exit plan can include a number of scenario plans with associated governance considerations and risk assessments.

For an exit that takes place in a planned, managed way, we have outlined below the high-level steps we would follow, as per our existing ISO 27001 / ISO 9001 compliant policies and procedures.

- Receive written confirmation of decision to exit / end contract from client.
- Fortesium and client to agree timeframes for exit.
- Fortesium, client and, if necessary, the new supplier, to discuss and agree the scope and format of data to be transferred. If a database back-up is to be provided, a timeframe for review and download / transfer of the data will be agreed with client.
- Fortesium to draft an exit plan including key activities, roles and responsibilities, and milestone dates.
- Fortesium and client to agree and formalise exit plan – include any other relevant stakeholders.
- Enact exit plan as per agreed schedule

Service Levels / Support and Maintenance / After Sales Support

We provide real, trained, and experienced people to deal with technical and functional support issues and queries from 09.00 -17.00 on all standard UK working days. Critical out-of-hours support can be provided based on the requirements of the client to cover critical calendar points.

Out-of-hours support will be resourced by the established support team, providing reassurance that any issue would be resolved promptly by Fortesium personnel with a detailed knowledge of the client's specific processes.

Support tickets can be raised easily in a number of ways via:

- The support portal
- Telephone – useful if you experience a power outage or connectivity issues. Our team will log a ticket on the portal for tracking and audit purposes
- Email

All tickets are recorded and tracked using a dedicated system to support prompt resolution and senior oversight of issues arising. This collation of support issues also allows us to identify themes and trends across clients that may warrant consideration as part of our continuous improvement cycles.

User requests are prioritised according to the agreed level of service in the SLA. Our support process enables the monitoring of each service request and progress against it. This proactive approach will ensure requests are completed on time and we both meet and exceed your expectations through the proposed Key Performance Indicators.

Our operating principles are:

- A single point of contact throughout the working day
- A prompt and effective response in line with our agreed SLA
- Recognition that individual requests must be met in an individual manner
- Effective management controls and escalation procedures

Typical SLAs for our support desk are outlined below but bespoke arrangements can be discussed and agreed as appropriate.

Classification	Description	SLA for Solution identification
Critical (L1)	Prevents core part of the system from working, there is no workaround.	2-hour response. Fix within 4 hours
Major (L2)	There is a difficult workaround.	4-hour response. Fix within 48 hours
Minor (L3)	There is an easy workaround.	8-hour response. Fix within 72 hours

Outage and Maintenance Management

We use an ISO27001 compliant Security Incident and Event Management (SIEM) tool to identify threats and recommend actions. The tool adds a rating to each threat to support assessment of the risk as it applies to Fortesium. We also conduct regular internal and external pen testing to identify threats and vulnerabilities. Our team take action to resolve or mitigate vulnerabilities in line with the risk rating attached to the issues raised.

We are subscribed to the National Cyber Security Centre (NCSC) to receive regular threat reports which alert us to new and emerging threats.

Solution updates may happen with varying frequency in response to new threats or vulnerabilities that we become aware of, or in response to a client specific defect or a defect that has the potential to impact all clients. Our clients will always be given due notice of a planned update via the Customer Success Manager or Service Desk and a plan made to ensure the update does not have a business impact.

Security

Fortesium is accredited with ISO27001:2022 (Information Security Management Standard) and as such we have a wealth of robust security procedures in place to protect the software application. Additionally, Regulator Online is Cyber Essentials Plus certified. A comprehensive list of security procedures and risk management processes can be made available on request.

Transport Layer Security
Data is fully encrypted in transit; this is enforced at all times for all connections and ensures that any data in transit between client and server is fully encrypted.
Transparent Data Encryption

SQL Azure Regulator Online ensures that all databases, backups and logs at rest are fully encrypted using TDE. Backups are stored, fully encrypted, in read-access geo-redundant storage (RA-GRS).