HEADER

ICAEW Technical Accreditation Scheme
"Governance, Risk & Compliance" Software Evaluation

FinReg GLOBAL

Date completed: 13th December 2023

CONTENTS

Ref		Vendor Comments	
1.	**INTRODUCTION AND PROLOGUE**		
Introduction			
1.01	The suitability of software for each particular user will always be dependent upon that user's individual requirements. These requirements should therefore always be fully considered before software is acquired. The quality of the software developers or suppliers should also be considered at the onset.		
1.02	Fundamentally, good software should: 1. Be capable of supporting the functions for which it was designed. 2. Provide facilities to ensure the completeness, accuracy, confidentiality and continued integrity of these functions. 3. Be effectively supported and maintained. It is also desirable that good software should: 5. Be easy to learn, understand and operate. 5. Make best practical use of available resources. 6. Accommodate limited changes to reflect specific user requirements. It is essential, when software is implemented, for appropriate support and training to be available.		
Approach to Evaluation			
1.03	The objective is to evaluate a product against a set of criteria developed by the ICAEW to ensure that the software meets the requirements of Good Accounting Software, as laid down in the summary.		
1.04	In order to effectively evaluate the software, a product specialist from the vendor completed the detailed questionnaire and provided it to the ICAEW to examine. The ICAEW's Scheme Technical Manager then reviewed the operation of the various aspects of the software assisted by a member of the vendor’s technical staff and checked the answers to confirm their validity. The questions were individually reviewed and commented on and the majority of assessments were confirmed.		
1.05	The Technical Manager discussed the assessment with a member of the vendor's staff in order to clarify any points requiring further information. In the event of disagreement between the supplier and the Technical Manager, the Technical Manager's decision was taken as final and the response changed accordingly.		
1.06	The latest version of the software was used throughout the evaluation.		
1.07	When the evaluation had been completed, a draft copy was sent to the ICAEW Scheme Manager for review before completion of the final report.		
Prologue: Matters to consider before purchase			

Ref		Vendor Comments	
1.08	General Overview:	FinReg Global Solutions develops and delivers high quality, robust and auditable sector specific Governance, Risk and Compliance (GRC) software solutions. FinReg's Technology Platform delivers Elegant GRC software solutions that: - Educates……. staff on the requirements - Enables…..teams to respond as required - Evidences…..your decisions, actions and compliance - Evolves……with an ever-changing regulatory landscape Tailored to meet a firm's System of Quality Management (SOQM) needs, QMCore tackles ISQM 1's quality challenges head-on. Equipping Audit Leaders and their firms with the right methodologies and tools, it navigates the complex ISQM 1 landscapes with a balance of flexibility and consistency. QMCore assists in managing the diverse quality requirements, and effortlessly adapts to a firm's business and regulatory circumstances, whilst streamlining the quality process from risk assessment through to monitoring & remediation. QMCore delivers elegant software that Educates workforces, Enables staff and Evidences compliance, via a centralised intuitive system	
1.09	Supplier background:	FinReg Global was set up in 2017 by Partners at EisnerAmper Ireland (a full service accounting firm and part of the EisnerAmper Group) to address a key issue in the market, namely that tech firms were trying (and often failing) to address complex Governance, Risk and Compliance (GRC) issues with tech solutions. The common reason of failure was an over reliance on tech without a proper understanding of the non-tech technical issues around GRC. The in depth inherent understanding of the subject matter experts, regulators or advanced users is essential to solving GRC issues and FinReg puts them at the centre of our solutions. FinReg has developed a cloud hosted proprietary technology Platform - The "FinReg Technology Platform" that enables subject matter experts and other relevant professionals to collaborate with product builders and the FinReg collaboration team to deliver GRC software (products) that address specific sector or cross sector needs.	
1.09 Cont…		This is enabled through a low-code/no-code solution and unlocks the delivery of quality focussed subject matter expert designed solutions for GRC - our designed for purpose products. FinReg's Technology Platform has enabled the delivery of Elegant GRC software solutions in: - Professional Services - Financial Services - Healthcare - ESG	

Ref		Vendor Comments	
1.10	Product background and suitability for the user:	QMCore is software built by subject experts specifically to meet a firm’s System of Quality Management (SOQM) needs. It addresses the quality challenges associated with ISQM 1 and provides the methodologies and tools required by Audit Leaders to manage and streamline the quality process from risk assessment through to monitoring & remediation. It provides consistency and flexibility whilst aiding the navigation of the complex ISQM 1 arena. It has been designed and built to adapt to your firm’s business and regulatory circumstances and adapt as they do. QMCore features provide: - a centralised location to capture and document all elements of a SOQM (from Risk Assessment through to Monitoring & Remediation); - the ability to capture key aspects of the firm and its services which impact the Risk Assessment process; - intuitive and user friendly Risk Assessment modules - facilitating the mapping of objectives to risks and responses, with all mapped risks available to re-use;	
1.10 Cont…		- pre-loaded mandatory objectives and specified responses mapped back to the requirements of the standard; - an indicative Risk library which can be tailored and configured for the nature and circumstances of your firm; - a Monitoring & Remediation regime (ResponseEMAR) allowing organisations to capture, assign, execute and report on the activities completed during each period including: - identifying monitoring that's completed, the testing approach and the execution; - capture findings and deficiencies from the monitoring; - create, document and manage the completion and review of Remediations; and - facilitate regular reporting to key stakeholders. - decision trees reflecting the nature, scale and complexity of an organisation; - dashboard reporting and exportable reports to facilitate an entities preferred reporting approach (PDF, excel, word); and - role assignment and task management to assist in the assignment of responsibilities, and tracking the progress of work completed.	
1.11	Add-on modules:	QMCore is an end to end solution for ISQM 1 (or relevant jurisdictional equivalent) demonstrable compliance. No specific add on modules are required. Organisations may request bespoke / tailored modules based on existing manual processes.	

Ref		Vendor Comments	
1.12	Typical implementation [size]:	The FinReg Technology Platform is highly scaleable and is designed to be suitable for use by any size of professional services firm. Access to the platform is managed by the Customer through a designated "Organisation" throughout the lifecycle of the product. The product has been built to facilitate the required data capture for all size firms. No installation is required - User access can be added once the initial onboarding of the Organisation administrator is completed (30 minute session).	
1.13	Vertical applications:	There are no vertical applications as QMCore is an end to end solution. The FinReg Technology Platform can facilitate seamless configuration through its low code / no code infrastructure. This infrastructure also facilitates bespoke requests from clients including new module builds and data ingestion modules.	
1.14	Server flatform and database:	The FinReg Technology Platform is a hosted solution, using AWS public cloud services. The Customer does not need any additional servers or databases.	
1.15	Client specification required:	Only basic information is required to set up a new Customer - the Firm name and an initial user email address (for the Organisation Administrator). Some additional Firm information may be required for the completion of the licence agreement. The FinReg Technology Platform can be accessed via all modern web browsers.	
1.16	Partner network:	N/A	

Ref				
2.	**ISSUES AND CONCLUSION**			
Highlighted issues				
2.01	**There are a number of limitations in the product, which while not adversely impacting upon this evaluation may be of importance to some organisations. It is important that any business contemplating the purchase of software reviews the functionality described and limitations therein against its detailed requirements. Attention is drawn in particular to the following areas where the product, on its own, may not be suitable for businesses with certain requirements:**			
2.02	Findings for considerations by potential customers: (See vendor comments against the various Questions)			
*	No SSO but this is currently in development.			3.08
*	Whilst data replication and backups are in place for the whole platform, backups/restores for individual customers cannot be undertaken in isolation.			3.28
*	There is no internal report generator. However the platform has standard reports and configuration of reports is available, with the ability to build customer-specific reports in Word.			4.30-4.37
*	There is no universal search facility; but filtering is easy.			5.15
*	The user manual/help is not editable by the end-user.			5.22
*	ESCROW is not offered; which is not unusual for this type of software as a service platform.			5.23
*	Service Credits are not offered should an anticipated service SLA not be met; but no SLA is explicitly offered.			5.33 6.28
*	There is no guarantee provided relating to service availability.			6.28
*	It is not possible for a customer to take their own backups.			6.51
*	Users are not able to test new versions before they go live. Note that this is not uncommon for SaaS platforms.			6.62
*	Firms cannot be linked but compliance would likely need to be undertaken separately.			7.22
*	Can roll forward an existing library within an organisation but not copy a library between organisations.			7.41
Evaluation conclusion				
2.03	For the specific use-cases in support of assisting accountancy firms to meet their own regulatory compliance requirements, for which the product is designed, it is a solid and capable solution. It continues to be actively developed and enhanced. Members should be aware of the limitation of the solution as above, and fully understand the role that it can play in helping manage their compliance needs. * NOTE THAT THE QUESTIONNAIRE RELATES TO THE SOFTWARE PRODUCT AND NOT ANY SUPPLEMENTARY SERVICES PROVIDED BY THE SUPPLIER TO THE ACCOUNTANCY FIRM USING THAT PRODUCT *			
Disclaimers				
2.04	Any organisation considering the purchase of this software should consider their requirements in the light of proposals from the software supplier or its dealers and potential suppliers of other similarly specified products. Whilst the contents of this document are presented in good faith, neither ICAEW, nor the ICAEW's Technical Manager (RSM UK Consulting LLP or any party nominated by the ICAEW to perform this role on the ICAEW's behalf) will accept liability for actions taken as a result of comments made herein. The decision to purchase software resides entirely with the organisation.			

Ref	Requirement	Vendor Response	Reviewer Comments
3.	**ACCESS AND SECURITY**		
Access control			
3.01	What security features are included to control access to the application?	Users are created via entering a valid email address. Each Users access is managed via a valid email address and password combination. Users can also be required to register a device for multi factor authentication purposes. Single Sign-On ("SSO") is currently in development. Once an email address has been added, the Users access is managed by the Organisation Administrator. The Organisation Administrator has the ability to: - Increase Group Role access to increase access / permissions; - Reduce Group Role access to decrease access / permissions; - Revoke User access - removing the Users access from the Organisation; or - Delete Users - This option is only available where the email address is not contained in an audit trail of a solution. All Data is encrypted at rest (KMS). HTTPs requests are protected from known bad IP or other WAF (Web Application Firewall) restrictions (e.g. rate limits), geolocation. Network traffic is inspected for suspicious behaviour (FlowLogs and GuardDuty). Privileged access to the database requires VPN	Noted
3.02	Can access to functions be managed via a permissions matrix so users can only see (in menus and other links) and access those areas they are authorised to access?	User access is based on email addresses. Each Users access is based on being added to an Organisation on the platform (unit of tenant isolation). Once part of an Organisation the level of access of a User can be controlled by Group access. Group access can be configured to provide access to features of the platform and access to data. See 3.01 above. Access to data is product specific and can be controlled at a very granular level (e.g. a User can only access data based on product sections they have been provided access to). Access to data in a product can be added and removed through removing a User from the "Task" associated with the data or by removing the User from a "System Group Alias" which is connected to a Task associated with the data.	Noted
3.03	Is this access to the application managed by:- - Individual user profiles? - User groups or job roles?	Individual access is via the Users email address and personal password (See 3.01). Access is managed through User Group Roles for general access, and through access directly to a specific Product Instance (e.g. engagements or products).	Noted
3.04	Can a report be produced detailing all current users, their user groups if relevant, and their authority levels and/or access rights?	All users can be accessed via the "Manage Users" screen include their current groups.	Noted. Can be seen on-screen. FinReg can provide an Excel dump on request.
3.05	If menus can be tailored does the system limit the display of menu options to those for which permission has been granted for each user?	All menus are available only on the basis of the user access (e.g. a user will only see menus based on their access). Additionally some menus (normally table views) can be configured by users to tailor the columns in their view.	Confirmed

Ref	Requirement	Vendor Response	Reviewer Comments
3.06	Does security allow for access to be limited to: - Read only? - Read/write? - Read/amend/delete?	Access (including read/ write etc.) is defined in two ways: - read only, read / write, read / amend access is defined based on Roles associated within a Product Instance (users can be added to a group providing different levels of access). Access to all Instances (and data) is based being in a role associated with Instance Task (and each task is connected to certain data) - All Group Roles (except Organisation Administrator) allow a user to edit data where they can access the data in an Instance. All write/amend/ delete actions at a data level is audited and available to the end user directly.	Noted
3.07	If data can be accessed by separate reporting facilities, such as ODBC or an external report writer, is the user access security control applied?	N/A - No external report writing, all reporting is on platform.	Noted
3.08	Does the system security integrate with Microsoft's Active Directory or other tools that provide a single sign-on?	SSO is currently in development and will ingerate with OKTA IAM and MS AD using the SCIM protocol	Noted
3.09	Does the system provide multi-factor authentication (MFA)?	Yes, 2 factor authentication is available and can be configured by the Organisation Administrator at an Organisation level, making it mandatory or optional for all Users in the Organisation.	Confirmed
Passwords and access logs			
3.10	Is access to the software controlled by password?	All users are required to manage and maintain a password with complexity and a minimum number of characters	Noted
3.11	Does each user have a separate log on (user id)?	All User access is based on a Users email address and password combination.	Confirmed
3.12	If there is no password facility please state how confidentiality and accessibility control is maintained within the software?	N/A	-
3.13	Are passwords masked for any user logging in?	Passwords are masked	Confirmed
3.14	Is password complexity available and enforced?	Passwords must be at least 8 characters. Passwords must have at least one non alphanumeric character. Passwords must have at least one digit ('0'-'9'). Passwords must have at least one uppercase and lowercase letter.	Noted
3.15	Are passwords encrypted?	Passwords are not directly stored within the FinReg Technology Platform, a one way hash system is used for security purposes.	Noted
3.16	Are users automatically logged off after a pre-set idle time? ~~not using the system?~~ - Can the time period be changed? - Can any information be viewed without being logged in, including after logging off, if so what information?	On set up of a user the session time out defaults to 15 minutes. This can be changed to a maximum of 60 minutes. On expiration, the Platform forces a User to log in again. If the browser session is still active the log out occurs when the user tries to interact with the platform. No password information is maintained by FinReg, but the User may choose to set their browser to remember access / passwords.	Noted
Deletion of transactions			
3.17	Is it possible to delete a transaction?	The FinReg Technology Platform records responses at a "Node" (e.g. Question & Responses) level based on the relevant requirements. Responses can be edited and amended and all changes are captured via audit trail. Transactions can be overwritten rather than deleted.	Not a transactional system. Questions can be "re-answered" if required.
3.18	If so, then how are deletions controlled by the system?	See 3.17 above.	As above
3.19	Are deleted transactions retained in the audit trail (see below) and denoted as such?	Yes, the deletion is based on a User re-setting or amending a previously answered node (at the transaction level). The audit trail records the original response and the amendment (or resetting) of the response.	Full audit history of any transaction is available on-screen.
Audit trails			

Ref	Requirement	Vendor Response	Reviewer Comments
3.20	Does the system have an audit trail (log) which records all changes to transactions in the system?	The FinReg Technology Platform records activities (write, amend, deletion) by users. Response activity audit trail is accessible on the front end by users. Full audit trail is maintained for all activities. Every Entity table in the Database has a corresponding Audit Table which records the changes to the entity, who they were done by and when they were done	As 3.19
3.21	Does this log also record any system error messages and/or any security violations?	System error messages and security violations are recorded within system administration tools such as those provided by FinReg's hosting partner, AWS. All API calls to the FinReg Platform backend are logged in AWS CloudWatch and all changes to the state of a Product, Product Definition, Product Instance or Actions related to a Product Instance are retained indefinitely in the Database as part of the FinReg Platform offering. All AWS API calls are audited by AWS CloudTrail and retained for 2 years in AWS CloudWatch.	Noted
3.22	Is it possible to turn off or delete the audit trail?	No the audit trail cannot be deleted. Users can "hide" the audit trail on their screen but all audit trail is still captured.	Noted
3.23	Does the software allocate a system generated sequential unique reference number to each transaction in the audit log, date and time stamp it and record the user id?	Sequential unique references are applied to all activities recorded in the audit log. The audit trail includes user id and time and date information.	Noted
3.24	Are all master file changes recorded in the audit trail?	N/A	-
Compliance			
3.25	Does the system operate in a way that is compliant with data protection legislation including GDPR? How does the system facilitate this?	FinReg have implemented a suite of policies and procedures in line with the requirements of GDPR. FinReg do not normally process or control Customer / User information except for: Customer billing and contact details and User contact information (emails) for the purposes of training and support. All users are added to the systems by the Customers Organisation Administrator (and by Users) via entering a valid email address. FinReg only add the initial email address for the Organisation Administrator. All information is stored by AWS on an Aurora Serverless Database. Access to the database is restricted to 3 Members of the management team. All access is logged via AWS logs and specific AWS role access. The database is not accessed by FinReg accept for support issues. Any other information added within an Organisation is "Customer Data" with the Customer acting as Controller of the data. All data is managed, processed and stored in accordance with relevant data protection laws with best in class security controls (technological and access based) in accordance with these regulations.	Noted
3.26	Describe your use of sub-processors if any?	The FinReg Platform uses AWS as part of hosting the FinReg Technology Platform. See link to Data processing terms: https://www.finregglobal.com/?page_id=1034 we also use Microsoft SharePoint for the storage of customer contracts.	Noted
Backup and recovery			
3.27	Is there a clear indication in the software or manuals as to how the data is backed-up and recovered?	Details regarding data backup and recovery are provided on request relating to AWS.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
3.28	How often are backups taken and to what point can restores be done?	Our database (Amazon Aurora Serverless) is built on a distributed, fault-tolerant, self-healing Aurora storage with 6-way replication to protect against data loss. Backups are continuous and incremental so we can quickly restore to any point within our 7 day backup retention period. No performance impact or interruption of database service occurs as backup data is being written Data replication is performed in real-time with point-in-time restores possible within a 5 minute window. Full weekly backups are also taken. It is not possible to customise this backup routine but software users are able to easily download transactional data for their own retention needs.	Noted. This applies to the whole platform. Backups/restores for individual customers cannot be undertaken in isolation. See also 6.48
3.29	How does the software facilitate recovery procedures in the event of software failure? (E.g. roll back to the last completed transaction).	Point in time restore to the previous restore point (<=5 minutes) within the redundant environment is automatic.	Noted
3.30	If software failure occurs part way through a batch or transaction, will the operator have to re-input the batch or only the transaction being input at the time of the failure?	The software user would need to re-input any information which had not been committed (i.e. written to the database) at the time of the outage.	Noted
3.31	What features are available within the software to help track down processing problems?	The FinReg Technology Platform includes detailed logging features that facilitates the engineering team identifying and understanding failures to re-produce the error to identify the required fix. The FinReg Platform is deployed using Fargate. Fargate deploys security updates and patches automatically based on the platform version. If a security issue is found that impacts a platform version revision, AWS creates an updated platform version revision and communicates the patch to FinReg, allowing FinReg to self-deploy but Fargate as a backstop automatic deployment.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
4.	DATA PROCESSING AND REPORTING		
Input and validation of transactions			
4.01	Is data input controlled by self-explanatory menu options?	Data inputs are supported with notes via Tooltips and Reference Documents containing links to supporting regulations.	Confirmed
4.02	Are these menus user/role-specific?	The FinReg Technology Platform records responses at a "Node" (e.g. Question & Responses) level based on the relevant requirements. Responses can be edited and amended and all changes are captured via audit trail. Access to edit/ input is based on user defined roles within a task. Where a user is not part of the task they cannot edit / input data and therefore cannot access menus. All access is based on the Users Group Role and Product Instance access which only shows the users information that they have been provided access to.	Noted
4.03	Can the creation or amendment of standing data (e.g. customer account details) be undertaken using menu options or dialogue boxes as opposed to requiring system configuration?	End user amendments are via the FinReg Technology Platform User Interface, these include User access changes, and inputs provided by the Users. Direct Product changes are managed by FinReg and released to customers e.g. for an update in relevant legislation.	Noted
4.04	Does the software provide input validation checks such as: - [account] code validation? - reasonableness limits? - validity checks?	All data input elements (except free text boxes) includes data validation e.g. decimals, vs. Integers vs. dates, valid email address format etc.	Noted
4.05	What control features are within the software to ensure completeness and accuracy of data input?	Data inputs can be qualitative and quantitative, where possible, validations of the accuracy or completeness of data inputs are completed as part of the product build and design.	Noted
4.06	How does the software ensure uniqueness of the input transactions? (i.e. to avoid duplicate transactions)	All data inputs are user defined. As the system is not capturing transactions no duplicate transaction testing exists	Noted. This is not a transactional system.
4.07	Is data input by users validated by scripts or routines in the browser, or other client software, before transmission to the server?	Where a product includes transactional data uploads, initial processing is carried out at the browser level to validate the data provided vs. validations for the data types. Further processing and validation in terms of calculations is carried out in FinReg's AWS environment.	Noted
4.08	Is data input by users validated by routines running on the server before data files are updated?	Data input is validated prior to the generation of the normalised dataset used in subsequent automated routines.	Noted
4.09	Does the above validation ensure that data entered in all input boxes: - Cannot be longer than a maximum length? - Cannot contain unaccepted characters such as semi-colons etc?	Where validations are included they are based on known / expected rules based on the data set or the inputs required for the Product.	Noted
4.10	Are responses to erroneous data input clear so that they do not lead to inappropriate actions?	Where data inputs do not meet the validation criteria based on the expected input, feedback is provided to the end user and the data is not recorded.	Noted
4.11	Does the software have an automatic facility to correct/reverse/delete transactions?	All data inputs can be re-completed with all activities (write, amend, delete) audited	Noted. Manual correction is possible.
4.12	If yes, are these logged in the audit trail?	Yes	Confirmed
4.13	Are all data entries or file insertions and updates controlled to ensure that should part of a data entry fail the whole transaction fails?	No partial fails are possible	Noted. This is part of the database integrity mechanism.
4.14	Are messages provided to users clearly explaining whether the data entry or file upload has been processed successfully or not?	Yes, the user interface shows the successful data input via the audit trail icon showing a green tick once successful.	Confirmed
Import and export of data			
4.15	Can files/attachments be uploaded and stored against any transaction?	Products include data upload nodes where users can upload information (e.g. attachments). It is not possible to upload data except to a data upload node.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
4.16	Is there an additional charge made for storage of uploaded files? - If yes, please indicate the cost.	No.	Noted
4.17	Can data be imported into the system from multiple types of files, e.g. XLS, text, CSV?	Data imports are based on the Product and normally are via excel or CSV.	Noted
4.18	Explain how the system validates imports into the system and what happens to any import which fails?	Data Imports (See above for general validations for data inputs) into the FinReg Technology Platform are normally based on a pre-defined data set and includes mapping to known source data providers. Where a data import does not match a provider for the required fields the data needs to be manually mapped by the user for each use. Where the data does not match a known provider the User can send the data to FinReg for further data validation. Imports that fail are not saved.	Noted
4.19	Are imported /interfaced transactions detailed in the audit trail? *[See also 3.27]*	N/A	-
4.20	Can data be exported from all areas of the system to multiple formats e.g. XLS, CSV, PDF, text; if so specify which formats are supported?	Yes data can be exported to excel. Word reporting is also available and visualisations are available in PDF format.	Noted
Data processing			
4.21	Does the software ensure that menu options or programs are executed in the correct sequence (e.g. outstanding transactions are processed before month end is run)?	The FinReg Technology Platform's QMCore solution is based on a workflow to capture the arrangements an organisation has in place, in line with the requirements of ISQM 1. As such the data inputs / imports are not traditional transaction based data. Where there is a logical flow to adding data the workflow and decision tree is configured to capture this.	Noted
4.22	Does the software provide automatic recalculation, where appropriate, of data input? (e.g. VAT)	N/A	-
4.23	Is a month/period-end routine required to be undertaken?	N/A	-
4.24	Is it possible to delete accounts if the balance is Nil but transactions have been recorded against the code?	N/A	-
4.25	What is the size and format of reference numbers and descriptions within:- - Ledgers? - Stock? - Currencies?	N/A	-
4.26	How does the software guard against/warn about duplicate account numbers on set up?	N/A	-
4.27	How does the software enable the traceability [from, to and through the accounting records] of any source document or interfaced transaction?	N/A	-
4.28	What drill down/around functionality is available within the software?	Where the data inputs from Users are captured and curated into a data set for visualisations, data underpinning the visualisation and graphs is available to "drilldown" into and where Users can view the data input source.	Confirmed. Easy drill down from dashboards and graphs.
4.29	If the software uses a lot of standing information which changes frequently or regularly, does the software allow for such changes to be effected through the use of parameters or tables?	N/A	-
Report writer			
4.30	Does the system have an in-built report generator or is a third-party solution used (if so please specify)?	Reporting is all via contained within the FinReg Technology Platform with no external solution required.	Noted
4.31	Is the report writer based on a standard SQL-type approach and is it flexible and easy to use?	Standard reports are available. Configuration of reports is available, with access to build Customer specific reports in Word available.	Noted
4.32	Can the report generator operate over the financial and operational aspects of the system, e.g. combining service metrics with financial information?	Reporting via excel is available across key aspects of the system. Access to operational and system reporting is based on Group Role Access.	Noted
4.33	Is a comprehensive data dictionary provided to aid field selection?	N/A	Noted
4.34	Does the system provide a library of reports and templates which can be amended, saved and re-run?	Yes	Confirmed

Ref	Requirement	Vendor Response	Reviewer Comments
4.35	Can users create their own reports? If so, what are the controls on users doing this?	Users can request to "write" their own reports however, standard reports are provided.	Confirmed. Template reports are provided. Users could change these themselves but usually FinReg would be asked to do this.
4.36	Can users create saved searches /filters / queries?	No	Noted
4.37	Can regular reports be added to user menus in the appropriate area of the system?	No	Noted
4.38	Does the system support the production of on demand (interactive) and scheduled batch reports?	All reporting is on demand, there is no scheduled batch reporting.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
5.	**USABILITY**		
Ease of use			
5.01	Does the solution provide a multi-language user interface?	The Platform is available in English	Noted
5.02	Does the system allow for customizable branding and UI (e.g. corporate colour palate, upload company logo, etc)?	White labelling of logo and primary and secondary colours on the Platform is available, per Organisation.	Confirmed
5.03	Does the system have a similar look and feel and overall and consistency between screens and modules?	Yes, consistency of symbols for features and functionality, with ability to navigate from the main task page and white labelling colours applied across the Organisation.	Confirmed
5.04	Is data entry easily repeated if similar to previous entry?	The FinReg Technology Platform has several different features to manage data re-entry including linking entries and re-using linked entries. Year-on-year cloning is available based on Product requirements.	Noted
5.05	Does the software prevent access to a record while it is being updated?	The FinReg Technology Platform records responses at a "Node" (e.g. Question & Responses) level based on the relevant requirements. The FinReg Technology Platform prompts users where two individuals seek to update the same Node at the same time.	Noted
5.06	Is there locking at file or record level?	All activities (write, amend, delete) at a Node level are saved and audited every time an activity is completed by a User. Access to edit data in a Product is via the "Task" associated with the Node. When a user has responded to all Nodes related to a Task, the Task status can be changed to "Complete". When a Task is complete the related nodes are made read-only. To make further edits, the related Task status needs to be updated back to "In Progress". Where a Task is subject to a Review workflow after it is prepared, completing the prepare Task activates the review Task. When a Node has been reviewed the prepare Task cannot be re-opened (this is configured by Product). Once all Tasks (preparer and reviewer) associated with an Instance are completed the Instance can be locked. Access to unlock an Instance is based on Group Role access.	Confirmed
5.07	Does the software allow for the running of reports whilst records are being updated?	All records are updated in real time, running of reports is completed based on the records completed at the time of running the report.	Noted
5.08	Can timestamps or user comments be added to transactions?	Each response on a Node is audited (time stamped and user ID) automatically by the FinReg Technology Platform. Comments can be added to each individual Node.	Confirmed
5.09	Is there the ability to store preferences and default values on a per-user basis. e.g. department/team/user?	The FinReg Technology Platform has a number of user defined preferences within the "My Account" section. Some security related preferences are configured at an Organisation level.	Confirmed
5.10	Does the system have the ability to provide user-defined fields with associated validation of data input?	N/A	Not a transactional system.
5.11	Can the system provide users with reminders and notifications e.g. workflows?	Access to edit data in a Product is via the "Task" associated with the Node. All tasks include email notifications which are sent prompting a user to log into the FinReg Technology Platform.	Confirmed
5.12	If the system provides workflows, does it have functionality to substitute/delegate authorisations?	Users can delegate "Nodes" using the Task Delegation feature	Confirmed
5.13	Is there the ability for users to define and configure layouts of letters and forms?	N/A	-
5.14	Can users save the parameters of searches?	No, searches clear after navigating away from the screen. Task Screen includes filters which can be saved.	Noted
5.15	Does the system have a "universal search" option, allowing a search to be undertaken over all modules of the system?	No	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
5.16	Can the system store menu option 'favourites' on a per user basis?	The FinReg Technology Platform includes some user specific options, allowing the user to create preferences.	Noted
5.17	Can a user open multiple windows accessing the same or different modules of the system?	Yes, this is possible by a User within the same Organisation. A user cannot be logged into multiple Organisations in multiple windows at the same time, unless they are using different browsers.	Noted
5.18	Can more than one software function be performed concurrently?	Multiple Users can access multiple sections of a single Instance and work concurrently. Each individual node can only be accessed and updated by one user at a time.	Noted
User documentation and training			
5.19	Is the manual provided as: - hard copy - on CD - by download - via a web-interface?	Hard copies can be provided and a copy is hosted on the platform.	Noted
5.20	Does the manual include: - An index or search facility? - A guide to basic functions of the software? - Pictures of screens and layouts? - Examples? - A tutorial section? - Details of any error messages and their meanings?	Manuals includes step by step guidance on using the product in question. FAQs are available on the Platform. All manuals include screen shots and details on using the features of a Product.	Noted
5.21	Is context-sensitive help available within the system?	Yes, tooltips are available and reference documents are included which link directly to the relevant regulations	Confirmed. Flexible having both tooltips and referenced documents together.
5.22	Is the manual and/or help editable by the user (subject to the permissions matrix)?	No	Noted
5.23	Will the Software House make the detailed program documentation (e.g. file definitions for third party links) available to the user, either directly or by deposit with a third party (ESCROW)?	No	Noted. This is not unusual for a SaaS platform.
5.24	Please detail the training options available?	Training and support is provided via remote sessions. Initial training is included as part of licence arrangements	Noted
5.25	Who provides training: - Software House? - VAR?	FinReg Global in-house product teams	Noted
Support and maintenance			
5.26	How is the software sold: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	The FinReg Technology Platform products are sold via FinReg global directly in the UK market.	Noted
5.27	How is the product supported: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	FinReg Global in-house product teams	Noted
5.28	Do VARs have to go through an accreditation process?	N/A	-
5.29	Is the software sold based upon number of named users or a number of concurrent users?	FinReg product licencing models are product specific. Product licencing is normally based on number of "Instances" of the product required.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
5.30	The supplier should detail the support cover options available, covering: - The hours provided? - Associated costs? - The global regions covered?	See SLA terms below: - Support hours during normal working hours 9.00 to 17.00 Irish Standard Time (IST) Monday to Friday, excluding Republic of Ireland bank holidays. • Support is provided via the Request Support page located on the Platform under the Help menu. All requests for support are initially submitted via the Request Support page with subsequent correspondence completed via email (support@finregglobal.com). • Standard response times for queries is within 48 hours. • Planned down time will be communicated at least 48 hours prior to the occurrence of the downtime. Where possible any planned downtime will be scheduled outside of normal working hours. Licence agreements identify annual support costs. Additional support hours can be requested and agreed with each individual customer.	Noted
5.31	Detail the process by which customers raise support requests and how these can be viewed/managed?	Post initial submission queries are managed via email	Noted
5.32	Please note the methods of support available: - Telephone? - Internet chat? - Remote access to customer workstation? - Other, please specify?	Initial query is via email with troubleshooting and resolution being via online video calls.	Noted
5.33	Do you offer service credits for failure to meet performance around SLA and uptime (if applicable)	No	Noted
5.34	What is your escalation path for tickets which have not been resolved within a reasonable time?	All tickers are managed and monitored by a member of the management team to resolution.	Noted
5.35	How often are general software enhancements provided?	Releases to the FinReg Technology Platform are based on expected weekly release cycle.	Noted
5.36	Will they be given free of charge?	Releases are not charged	Noted
5.37	How are enhancements and bug fixes provided to customers?	All bugs and fixes are released by FinReg to the cloud hosted environment.	Noted
5.38	Is “hot line” support to assist with immediate problem solving available?	No. All queries are prioritised and actioned accordingly	Noted
5.39	If so, is there an additional cost involved?	N/A	-
5.40	At what times will this support be available?	N/A	-
Integration and www facilities			
5.41	Can the software be linked to other packages e.g. word processing, graphics, financial modelling, to provide alternative display and reporting facilities?	Data can be exported via excel downloads and word based reports allowing for the use in external solutions.	Noted
5.42	Can definable links to spreadsheets be created?	Adding of links to any source is supported. Creating data links is not supported	Noted
5.43	Does the system provide a secure document storage capability: If so, please give examples of the document types saved and what transactions these might relate to.	Documents can be added by users. The FinReg Technology Platform uses AWS S3 buckets for document storage	Noted
5.44	Can documents be scanned into a secure repository?	Direct document scanning is not supported. PDF scans can be uploaded	Noted
5.45	Does the system provide data migration tools for transactional and master data sets (e.g. employees customers, suppliers, journals, invoices).	Migration can be supported through downloading of data into excel	Not a finance system.
5.46	What connection mechanisms does the software have and what breadth of functionality in terms of: - operations (add, update, delete)? and - what transactions/data it can access? E.g. if webservices APIs available, then can customers connect to whatever software they wish?	The FinReg Technology Platform consists of over 200 APIs. All functionailty available on the Platform is available through these APIs.	Noted. Integration with third-party APIs are available on request.
5.47	Does the system support mobile working?	As a cloud based solution the platform supports mobile working although it tailored for laptop/computer use and not for mobile/tablet use. For security purposes the system does include Geo Location protection.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.	**SAAS/HOSTED OPERATION**		
	This evaluation covers the system but not the method by which it is delivered and/or contracted for. Potential users need to satisfy themselves on the security and disaster recovery aspects and licensing of the online system and any data protection issues of their own and customer/supplier information, contained therein, being held on the system, as well as the return of the data when the contract expires or is terminated.		
Data centres and customer data			
6.01	Whose data centres are used and where are these located: - If hosted -- where data centre controlled by a third-party? - If SaaS -- where the software vendor will be in control?	The FinReg Technology Platform is hosted by AWS using their multi-tenant platform. UK: eu-west-1 (Ireland) Ireland: eu-west-1 (Ireland) USA: us-east-2 Singapore: ap-southeast-1	Noted
6.02	Does the customer get a choice of the jurisdiction in which their data resides?	FinReg currently offers the regions noted in 6.01 above, a dedicated UK based location can be added for UK clients (eu-west-2).	Noted
6.03	What certification(s) do you or your platform operators hold relating to your data centres and your business operations?	FinReg is ISO 27001: 2017 certified and currently awaiting receipt of finalised SOC 2 Type 1 report assessment. A SOC 2 Type 2 report will be available in 2024. (https://www.finregglobal.com/wp-content/uploads/2022/10/FinReg-Global-Solutions-Limited-NSAI-Cert-2022.pdf) AWS computing environments are continuously audited, with certifications from accreditation bodies across geographies and verticals, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70), SOC 2, SOC 3, ISO 9001 / ISO 27001, FedRAMP, DoD SRG, and PCI DSS Level 1.i. https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf https://aws.amazon.com/compliance/programs/	Noted
6.04	Do you or your platform operator have an SSAE16 (System and Organization Controls) report available?	Currently awaiting receipt of SOC 2 Type 1 report	Noted
6.05	What are the physical controls over the:- - Premises? - Fileservers? - Communications equipment?	AWS provide industry best practice physical controls consistent with their certifications.	Noted
6.06	Is the space in this/these data centre(s) shared with any other companies?	Yes - See AWS data center controls https://aws.amazon.com/compliance/data-center/controls/	Noted and see 6.07, 6.08 and 6.09
6.07	Is data for different customers/companies kept:- - On separate servers? - In different databases? - In separate database tables? - In a database with data for other customers and companies using logical security to partition customers' data?	Data is partitioned via logical security. FinReg have applied the AWS Well Architected Framework, AWS best in class cloud architecture. The FinReg Platform is a multi-tenant platform. · The unit of tenant isolation is the Organisation. · Users can belong to more than one Organisation but they can only ever be signed into a single Organisation at a time.	As above

Ref	Requirement	Vendor Response	Reviewer Comments
6.08	How is it ensured that data for different customers and companies is reliably identifiable and only accessed by authorised users for each customer/company?	The FinReg Platform is a multi-tenant platform. The unit of tenant isolation is the Organisation. Users can belong to more than one Organisation but they can only ever be signed into a single Organisation at a time. User access is based on user email address. Each users access is based on being added to an Organisation on the platform (unit of tenant isolation). Users are created via entering a valid email address. Each users access is managed via a valid email address and password combination. Users can also be required to register a device for multi factor authentication purposes. SSO is currently in development. Once a User has been added to an Organisation, and accepted the invitation, their access is managed by the Organisation Administrator. See 3.01 and 3.02 for more information.	As above
6.09	What controls are in place to prevent users from one customer/company accessing data from another customer/company by accident or by design?	The FinReg Platform is a multi-tenant platform. The unit of tenant isolation is the Organisation. Users can belong to more than one Organisation but they can only ever be signed into a single Organisation at a time. During sign in the User must pick which Organisation to access for this session. User access is based on user email address. Each users access is based on being added to an Organisation on the platform (unit of tenant isolation). Users are created via entering a valid email address. Each users access is managed via a valid email address and password combination. Users can also be required to register a device for multi factor authentication purposes. SSO is currently in development. Once a User has been added to an Organisation, and accepted the invitation, their access is managed by the Organisation Administrator. See 3.01 and 3.02 for more information.	As above
6.10	How is [Internet] communication traffic monitored to identify potential problems before they happen: - From a performance perspective? - From a security standpoint?	FinReg's AWS infrastructures makes use of AWS's Web Application Firewall which protects the platform and users against common web exploits with Amazon CloudWatch implemented to monitor and reporting on traffic metrics. Network traffic is inspected for suspicious behaviour using AWS FlowLogs and GuardDuty.	Noted
6.11	What procedures are in place to prevent a break in Internet Connection (at the server, client or in between) from causing data corruption?	Data is either accepted immediately by the server or rejected entirely. It is not possible to accept a partial upload.	Noted
6.12	Are communications between the user's computer and the software service encrypted: - User log in data only? - All data exchanged between user client and software service?	All Data is encrypted at rest (KMS). Data is encrypted in transit using HTTPs over SSL. This includes any data sent across the company network and the public internet, or any data sent to or from a company-owned or company-provided system. The platform applies 256-bit AES encryption for transmission.	Noted
6.13	Is data on your servers encrypted at rest?	Data is encrypted at rest using AWS KMS Encrypt API using 256-bit AES.	Noted
6.14	Is a test environment provided to test configuration changes? If so, is there an additional charge for this?	FinReg can arrange access to a non-production environment or organisations to facilitate configuration and testing (if applicable).	Noted
Access to customer data			

Ref	Requirement	Vendor Response	Reviewer Comments
6.15	What are the implications of the Data Protection Act over information held by the hosting service provider, and how does the vendor mitigate these?	FinReg have implemented a suite of policies and procedures in line with the requirements of GDPR. FinReg do not normally process or control Customer / User information except for: Customer billing and contact details and User contact information (emails) for the purposes of training and support. All users are added to the systems by the Customers Organisation Administrator (and by Users) via entering a valid email address. FinReg only add the initial email address for the Organisation Administrator. All information is stored by AWS on an Aurora Serverless Database. Access to the database is restricted to the Head of Operations and Head of Engineering. All access is logged via AWS logs and specific AWS role access. The database is not accessed by FinReg accept for support issues. Any other information added within an Organisation is "Customer Data" with the Customer acting as Controller of the data. All data is managed, processed and stored in accordance with relevant data protection laws with best in class security controls (technological and access based) in accordance with these regulations.	Noted
6.16	Are you subject to any legal or regulatory requirements obliging you to retain a copy of customer data?	FinReg are subject to legal and regulatory requirements as an Irish incorporated entity. Examples include GDPR, EU Directives, Irish Company Law etc. FinReg are not subject to any specific legal requirements to maintain "Customer Data" other than information connected to financial reporting obligations.	Noted
6.17	Who will be able to access or see customer data?	Customer data can be accessed by Customer Users based on the Groups and permissions provided to the Users. User groups may provide access to both functionality and data. FinReg do not have access (except via direct access to the database) to customer data. FinReg, via a System Administrator role, can access user information (first name, last name and email address) and the instance name and Owner information for support and maintenance purposes. FinReg cannot access the Product data unless they have been invited to be part of an instance to provide customer support.	Noted
6.18	Explain the procedures to prevent unauthorised access from staff, or contractors, working for the service provider or any other people with access to the service provider’s internal systems.	Access rights are assigned to FinReg staff based on individual roles. Currently System Administrator access is restricted to Head of Operations and Head of Consulting. No other staff have privileged access to the Platform. In line with ISO 27001, FinReg maintain and regularly review all access of staff to ensure "least privileged access". (see 6.15 re access to AWS). FinReg additionally have procedures and controls relating to off-boarding staff. Physical access controls are in place within FinReg's office environment.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.19	Explain the release management procedures in place and the associated segregation of duties ?	All releases are managed by the Release Manager and are overseen by the Head of Engineering and Head of Operations. The development and release procedure process is managed using Atlassian Jira. The release procedure includes a number of steps including code review, UAT and regression testing on both local, testing environments. The engineer who prepares the code, is not allowed to code review or test it, and the regression testing script is run by the Release Manager. Releases to Production environments are completed by Head of Operations, on confirmation from Head of Engineering and the Release Manager that all testing has passed and the release can proceed.	Noted
6.20	Is there sufficient segregation of duties preventing system developers from accessing and changing live applications and data files?	The Engineering Team do not have access to release to AWS, or System administrator access on the Platform. The Platform administration duties are completed by the Product team in FinReg and not the Engineering Team. Customer data cannot be changed by FinReg.	Noted
6.21	Explain the review and approval procedures covering system operations staff when emergency changes need to be made to live applications and data?	All releases are subject to UAT and Regression Testing. Releases are completed outside of business hours, unless an urgent fix is required. The full release procedure is completed for emergency changes to ensure no additional problems get introduced to the Platform.	Noted
6.22	Is an audit trail always maintained of these emergency changes?	An audit log of AWS releases is available on AWS and a separate log is maintained and updated by the individual completing the release.	Noted
6.23	What procedures are in place when members of staff leave to ensure that their system access is stopped?	FinReg have a leavers procedure in line with ISO 27001 and this includes a leavers procedure checklist including removal of all access.	Noted
Platform and service levels			
6.24	Which databases can be used (Hosted) or are used (SaaS)?	AWS Aurora Serverless Database	Noted
6.25	What forms of user authentication are supported e.g. user names, passwords certificates, tokens etc.?	On creation of a user, a token is emailed to the user for initial login and password creation via a token which expires. Once a user account has been created (first name, second name, email address and password), subsequent sign in's are via email address and password. Customers at an Organisation level can enforce Multifactor Authentication. A SSO solution is currently in development.	Noted
6.26	What is the proposed product/service availability percentage?	AWS use commercially reasonable efforts for Monthly Uptime Percentage of at least 99.99999%	Noted
6.27	What percentage availability has been achieved over the past 12 months?	No known outages recorded in the past 12 months	Noted
6.28	Is a service level agreement ("SLA") offered regarding: - Service availability? - Data recovery?	AWS offer standard SLA for uptime and recovery, the FinReg licence agreement sets out SLA terms which includes commercially reasonable efforts for up time during business hours with agreed approach to expected downtime outside of standard business hours. https://aws.amazon.com/legal/service-level-agreements/?aws-sla-cards.sort-by=item.additionalFields.serviceNameLower&aws-sla-cards.sort-order=asc&awsf.tech-category-filter=*all	Noted
6.29	Is the service available 24x7 or are there downtime periods for maintenance?	Planned maintenance and downtime will be communicated in advance, and where possible completed outside of business hours excluding Platform critical bugs or errors.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.30	Is the customer made aware of maintenance periods in advance?	Planned maintenance and downtime will be communicated in advance in line with the Customer license agreement.	Noted
6.31	Does the application software:- - Require any client software to be installed on the user’s computer? - Work entirely within Internet Browser software on the user’s computer?	The platform is accessed via a supported internet browser (ECMAScript 6 or above), there is no installation required.	Noted
6.32	Where the product/service relies upon downloading and running an executable program, has that program been secured with a digital certificate to verify the source and integrity of the program?	Not applicable	-
Platform security			
6.33	What security steps are taken to prevent and detect intrusion attempts?	FinReg's AWS infrastructures makes use of AWS's Web Application Firewall which protects the Platform and Users against common web exploits with Amazon CloudWatch implemented to monitor and report on traffic metrics.	Noted
6.34	Is firewall hardware and software used to protect the live systems from unauthorised access?	FinReg's AWS infrastructures makes use of AWS's Web Application Firewall which protects the platform and users against common web exploits with Amazon CloudWatch implemented to monitor and report on traffic metrics.	Noted
6.35	Which monitoring software is used to create alerts when intrusion attempts are suspected?	Amazon CloudWatch implemented to monitor and report on traffic metrics.	Noted
6.36	Are designated staff responsible for receiving and urgently responding to these alerts?	CloudWatch notifications are sent to an alert group which can be accessed by Head of Operations, Head of Engineering and Head of Consulting. Head of Operations is assigned responsible to review and action alerts.	Noted
6.37	Have clear procedures been established for identifying and responding to security incidents?	Incident Management policy and procedures are implemented to manage incidents. Regular training is completed by staff related to security threats.	Noted
6.38	Is all security sensitive software, such as operating systems and databases, kept up to date with the latest software patches? Please indicate how regularly updates are applied.	FinReg's AWS infrastructure utilises the ECS application which manages all patches. Any required security patches to the operating system or data bases is managed via this by AWS.	Noted
6.39	List the procedures and software tools in place to prevent or detect and eliminate interference from malicious code, such as viruses?	FinReg's AWS infrastructures makes use of AWS's Web Application Firewall which protects the platform and users against common web exploits. Staff laptops are encrypted with BitLocker and Sophos Central Intercept X Endpoint Advanced with EDR is our cloud based endpoint protection to stop unknown threats, block ransomware, deny attackers. All files uploaded to the platofrm are scanned for Malware using Trend Micro Cloud One™ File Storage Security.	Noted
6.40	Is a system log maintained by the service provider that details - User access? - User activity? - Error messages? - Security violations?	AWS CloudTrail logs all Platform access directly within AWS. The audit trail within a Product tracks user activity within a product.	Noted
6.41	Is this log available to the customer?	The Cloud Trail log is not available to Customers, but the audit trail log is available per node.	Noted
6.42	Have there been any successful unauthorised access attempts been made during the last year? If Yes:- - What was the effect on the business and users? - What steps are in place to prevent this happening again?	No	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.43	Is penetration testing regularly carried out by (please indicate frequency of tests): - Staff specialising in this field? - External specialists?	FinReg engage an external firm to conduct penetration testing at least annually, with AWS specialists engaged to review, advise and implement updates to our AWS architecture and security. FinReg also have a customer who helps to test new and existing functionality before it is released.	Noted
6.44	If penetration testing by a specialist is not performed regularly, please indicate the main procedures in place to identify weaknesses?	N/A	-
6.45	Are security procedures regularly reviewed? Please indicate frequency of reviews.	All policies and procedures, in line with ISO 27001, are reviewed on an annual basis	Noted
6.46	What security reporting is provided demonstrating compliance against certification(s) and policy(ies)?	FinReg operate an internal audit and an external audit schedule to assess compliance with policies as part of ISO 27001. Additionally FinReg is subject to annual reviews in relation to SOC 2 reporting.	Noted
6.47	Are any security breaches communicated to customers?	Security breaches are communicated to affected customers (if any).	Noted
Backups by the service provider			
6.48	In relation to backups undertaken by the system provider please explain: - How is a customer's data backed up? - How often is this undertaken? - What is backed up? - What's the media used? - Where are backups stored? - How many copies are there? - How long are they retained for? - Who has access to them? - Is the data encrypted?	Our database (Amazon Aurora Serverless) is built on a distributed, fault-tolerant, self-healing Aurora storage with 6-way replication to protect against data loss. Backups are continuous and incremental so we can quickly restore to any point within our 7 day backup retention period. No performance impact or interruption of database service occurs as backup data is being written. All other data is stored on Amazon S3, an object storage built to store and retrieve any amount of data from anywhere on the Internet. It's a simple storage service that offers an extremely durable, highly available, and infinitely scalable data storage infrastructure at very low costs. All S3 buckets used to store user documents are created in CloudFormation with access control set to Private. Backups are managed by AWS with an expected durability of 99.999999999% of objects over a given year.	Noted. This applies to the whole platform. Backups/restores for individual customers cannot be undertaken in isolation. See also 3.28
6.49	How frequently is a test-restore of backups undertaken?	Test- restore is undertaken in line with internal policies and as deemed required	This is handled by AWS.
6.50	Can the provider restore from a backups that it has taken at a customer request?	No, the restore from back up is for the entire platform and would impact other Platform users.	Noted. See 6.48 above.
6.51	Does a customer have the ability to undertake their own backups?	No	Noted
6.52	If so, can a customer restore data a backup that they have taken?	Customer restoration from the excel download would be based on a manual changes.	Noted
Platform recovery			
6.53	What contingency plans are in place to enable a quick recovery from: - Database or application software corruption? - Hardware failure or theft? - Fire, flood and other disasters? - Communication failures?	The FinReg platform has been implemented using AWS Failover routing, which lets FinReg route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy. AWS Disaster recovery plan can be found here https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/business-continuity-plan-bcp.html FinReg utilise a Multi-AZ (availability zone) architecture as part of it's high availability strategy. Availability Zones isolate faults that could impact workload resilience, preventing them from impacting other zones in the Region.	Noted
6.54	How often are these plans tested?	All parts are tested at least annually, with some tests occurring more frequently.	Noted
6.55	How often are these plans reviewed and updated?	At least annually in line with ISO 27001	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.56	What are your: - Recovery Point Object (RPO) standards? - Recovery Time Objective (RTO) minimum standards?	Recovery Time Objective (RTO) is the maximum acceptable delay between the interruption of service and restoration of service. It is FinReg's objective that service is restored as soon as possible. Usually on notification of interruption of service an Engineer is immediately allocated to resolve the problem. Recovery Point Objective (RPO) is the maximum acceptable amount of time since the last data recovery point which is 5 minutes.	Noted
6.57	If transaction records are dated and time stamped are the times used local to the user or based on where the server is located?	All servers operate based on UTC with localisation available at a user level which converts the audit trail accordingly.	Noted
6.58	What protection is in place to enable users to able to access their accounting and other data if the service provider should experience serious difficulties, cease trading or decide to stop providing the service?	A minimum of 30 days will be provided by the hosting provider for the customer to download their data.	Noted
6.59	If the system is hosted are there arrangements in place for this third party to continue providing a hosting service in the short term to allow time for customers to negotiate their own arrangements? If so, how long does the arrangement allow?	30 days minimum is provided by AWS in line with their standard service agreement.	Noted
6.60	Are there any individual members of the vendor's staff whose leaving or illness would significantly reduce, or even stop, the service provider's ability to provide a full and reliable service to customers?	No	Noted
Platform change management			
6.61	Describe your approach to upgrades including what option customers have not to take upgrades (if any)?	Upgrades may be platform or product specific. Where upgrades are product specific, these are communicated and agreed with customers in advance where they result in a significant change. Product changes can be managed through the FinReg Technology Platform change management modules including in-situ migrations and EvoCon. Platform change / upgrades are applied by FinReg with no user ability to accept / decline. Where a platform upgrade changes the user experience this is communicated to the customer.	Noted
6.62	Are users able to test the application before new versions go into live use?	User testing is completed by FinReg with their development partners. Access by Customers is on the basis where a Customer has requested bespoke configuration.	Noted
6.63	Are users given notice before application changes are applied to the live system?	FinReg patch and make enhancements to the features and functions on the platform on a continuous basis. Any changes to features which impact the use of any Product is communicated in advance to the Customers assigned main point of contact.	Noted
6.64	Are changes delivered into the live environment "switched off" to enable users to test them before enabling them for their environment?	Only changes which are designed to be configurable by the user can be "switched off"	Noted
6.65	Describe what testing and QA processes are undertaken before upgrades and other changes are made live/available to customers?	Testing is completed on non-production environments by both FinReg staff and their development partners before the changes are made available to customers. Testing is completed for both Platform and Product changes with Head of Consulting confirming when Product changes can go live and Platform changes are confirmed in line with the release procedure.	Noted
6.66	If a hosted system, explain the release management procedures in place and the associated segregation of duties?	N/A	-

Ref	Requirement	Vendor Response	Reviewer Comments
6.67	Are users informed when they next login of the application changes that have gone into live use?	Users are informed of the update via a change in the version number, and are prompted to complete a "hard refresh" if they are not using the latest version. Changes can be seen in the "What's new" section on the Platform. Major changes to User experience are communicated to the Customer in advance with training provided if required. Users in an active session during an update are prompted by the system.	Noted
6.68	Do customer staff have to take any action (e.g. regression testing) when new editions, patches or upgrades are released? If so, please describe what they should ordinarily do.	No	Noted
Subscription options			
6.69	What is the minimum level of commitment must the customer sign up to, e.g. 36 months?	Minimum period of sign up is normally 36 months.	Noted
6.70	Where online payment is used, what type of security is used to protect sensitive information?	FinReg do not usually use an online payment provider but have an account with Stripe if required.	Noted
6.71	Where online subscription / payment is used, is an invoice provided to the customer and, if so, in what format?	PDF invoices and an online link of the invoice are sent to customers via email	Noted
6.72	When subscriptions need to be renewed, what advance notice is provided and what is the time limit for renewal?	Re-subscription can be arranged by the customer at any time based on signing of a new licence agreement. FinReg issue new licences in advance of end date in order to ensure continuity of service	Noted
6.73	Is there a procedure for late renewal and is there a time limit after which subscriptions cannot be renewed?	No specific procedures are in place but access to the Platform may be removed. Upon a non-renewal FinReg would contact client to confirm non-renewal and organise the return of their data.	Noted
6.74	How soon after creating or renewing a subscription (if applicable) can the system / service be used?	Access to the Platform is provided immediately upon payment	Noted
6.75	What notifications / confirmations are provided to the customer regarding subscriptions and payments?	Email confirmation are sent regarding invoices and licences	Noted
6.76	To what extent are users able to access their accounting and other data if: - They miss one or two payments? - They cease being customers?	In line with licence agreement, FinReg reserve the right to remove access on any non payment. In line with our licence Agreement, data retrieval may be subject to a data retrieval fee. A period is defined in the licence agreement where FinReg retain the data on cessation.	Noted
6.77	At the end of the contract term, how long does a customer have to obtain a copy of their data from you?	Data is archived and held for a period of up to six months unless otherwise agreed.	Noted
6.78	At the end of the contract term, how is a customer's data destroyed (if appropriate) and will that destruction be certified?	Full Deletion of the customers data will occur, with all backups of the data removed 7 days after the deletion is completed (allowing for the overwriting of back ups). Confirmation of deletion will be provided via email.	Noted
6.79	What is your processes regarding disposal of end-of-life and failed hardware devices that were used to operate your service?	FinReg have destruction policies in relation to hardware in line with ISO 27001 including removal and separate destruction of hardware storage. Customer data and Platform data is not stored on FinReg's hardware it is all cloud based.	Noted
SaaS/Hosted Reporting			
6.80	Are reports produced from the same software as the financial applications or is separate reporting software used?	Reports are generated directly from the FinReg Platform	Confirmed
6.81	Does any application software (i.e. other than a web browser or PDF reader) need to be installed on the user’s computer in order to prepare or view the reports?	No other software required	Noted
6.82	What browser versions are support: - On desktop/laptop (PC, Mac, Linux)? - On Tablets? - On mobiles?	Desktop / laptop fully supported using a modern up to date (for security) browser. The Customer must have high-speed broadband or another high-speed internet connection for proper transmission of the Platform. The Customer is responsible for procuring and maintaining the network connections and browser. The browser must be compatible with ECMAScript 6 or above.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.83	Is access to the reporting facilities and data controlled by the same procedures as access to the main application?	Yes, all reporting is based on User Group access	Noted
6.84	If it's different, explain the user access control facilities available to ensure information is only viewed by users with appropriate authority?	N/A	-
6.85	In what electronic formats are reports produced:- - PDF? - XML? - MS Excel spreadsheet? - CSV file? - As html for viewing in a web browser? - Other, please specify?	PDF, Excel, Word	Noted
6.86	Are report documents stored on the web server or on the user's computer? If stored on the web server, are they secure to ensure only users with appropriate authority can get access?	Dashboard reports can be viewed directly from the platform, other reporting is downloaded to the Users computer.	Noted
6.87	For documents viewable in a browser is any data stored on the user's computer in a web browser cache or temporary file? If Yes: - Is there any protection against other users viewing the report or data on which it is based? - Is it clear on the reports when they were produced and the date of the data on which they are based, so the user can tell whether they are viewing out of date information?	The dashboard reports that are viewed from the Users browser are **only** accessible to the Users who have been provided with the applicable Group User access. For PDF, Excel and Word reports it will be the Users decision whether to open them in a browser or directly from their computer. This is not controlled by FinReg.	Noted
6.88	Are communications between the browser and the server encrypted for any report related communications?	All communications are encrypted in transit and at rest.	Noted
6.89	If reports are produced dynamically each time the user views them can historical reports be reproduced at any time?	Reports are based on the current state of the product in question. The audit trail shows all actions. QMCore is an ongoing system of quality management and point in time reporting is not included.	Noted
6.90	Can reports viewable in a browser be navigated dynamically by users? For example: - Enabling drill down to more detailed information? - Altering which columns and rows of data are displayed. - Choosing time periods? - Specifying selection criteria?	Dashboard reporting is configurable by the User with drill down capability and editability. The dashboards can be created from any of the data that has been inputted by the User applicable to the Product.	Noted
6.91	Can report data be reliably copied and pasted direct from browser viewable reports to an MS Excel spreadsheet retaining any table layout?	All data is available to export to excel. It is possible in most cases to copy direct to MS Excel	Noted
6.92	If reports are incomplete, for instance due to a poor Internet connection, is sufficient information provided to enable the user to notice that some of the report is missing?	It is not possible to download partial reports and slow internet providers will cause the screen to be blank or have a loading icon on the screen.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.	**GOVERNANCE, RISK & COMPLIANCE**		
	Note that the phrase: • "Firm" has been used for the Entity or Firm of Accountants having individual "Users" of the software platform. • "Compliance Instance" has been used to describe a single Regulatory Compliance regime under which a Firm must operate or be compliant with, e.g. "SQSM1", International Standard on Quality Management 1 for firms that perform audits or reviews of financial statements or other assurance of related service engagements.		
Global configuration/setup			
7.01	Does the system provide for the setup and maintenance of the details of the Firm which has Users using the software?	QMCore includes an entity and environment section which allows Firms to document and update the nature, scale and circumstances of the Firm including key information relating to the Firm.	Confirmed
7.02	Does the system provide a permissions matrix so that rights can be set at User and role/group level?	Each User's roles can be partitioned based on their role / responsibility within the Organisation and the specific access that is required. Access to each section of the Product can be provided to the relevant Users.	Confirmed
7.03	Does this apply to: - Administration of access for the Firm's Users? - Specific areas of functionality? - An individual "Compliance Instance"? - A specific section within a "Compliance Instance"? - Manually adding/editing transactions [objectives/risks]? - Authorisations? - Access to any linked systems? - Other, please specify?	Access (including read/write/update/review etc.) is defined in two ways: - read only, read/write and read/amend access are defined based on Roles associated within a Product Instance (Users can be added to a Group that provides different levels of access). Access to all Instances (and data) is based on being in a role associated with an Instance Task (and each task is connected to specific data) - All Group Roles (except Organisation Administrator) allow a user to edit data where they can access the data in an Instance. All write/amend/delete actions at a data level are audited and available to the end user directly. Training is provided to the Organisation Administrator about the roles and the access they provide.	Noted
7.04	Does the system have the ability to set up accountabilities and responsibilities for compliance for named members of the senior management? If yes, how does the system support this?	The Firm can define key individuals within their system of quality management. The documentation of these roles is for reporting purposes only. Access for these individuals can be managed via the individuals User access controls noted above.	Confirmed
7.05	Can a separate user account be created specifically for a "regulatory body" and which provides read-only access to the data for audit/review purposes? If so, please explain what is provided.	Multiple user accounts can be created for regulators. Access to the data can be managed for each section including read/write/view access. Specific roles can be added for viewer only access through a request to FinReg	Confirmed
7.06	Does the system provide a way to capture feedback from a Regulator in a way that can be tracked, managed and assigned within the system?	The platform includes access to create events (which includes deficiencies, remediation and observations). Events are documented for reporting purposes. The Platform includes an "External Task" feature which allows for actions to be assigned and tracked directly on the Platform (including assigning priorities and due dates).	Confirmed. Events can be added.
7.07	Can users be "archived" if they are no longer active within the Firm? If so: - Is a history of the risk assessments that they worked on retained by the system? - Can they be "unarchived" to re-enable their access?	All Users account access can be revoked to remove their access. Any Users who interact on the FinReg Technology Platform (through answering questions) cannot be deleted in order to preserve the audit trail of actions completed. When a User account has been revoked access can be re-established with the User being prompted by the Platform.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.08	Is it easy to see what security level/profile a user is logged in as, e.g. is their users 'name' displayed on-screen? If so, can a user change profile [by logging in again] from a menu screen?	Once logged in each User can access a manage account section which details the user profile and settings. The Organisation Administrators can see all Users Group access and manage this access from the User administration screen. Reports on each users role and access within a Product can be requested from FinReg.	Confirmed. The user can see the account and instance that they are logged in as/using.
7.09	Is it possible to define delegated access? If yes then please explain the levels of access provided.	All interactions on the Platform are managed via tasks. Elements of tasks (e.g. a question/section) can be assigned to other Users which creates a specific task for the User to complete. Organisations can control if delegation of tasks can be completed for existing users only. Where delegation to non-existing user is allowed, any non-existing User is initially added to the Organisation with the lowest level of role access (Organisation Guest) required to access the information they have been assigned.	Confirmed
7.10	Can multi-level authorisations be set? E.g. A users and their manager must both approve an action?	Tasks can be added for both the preparation and review of actions. The review process between preparation and review tasks are automated with rejections of answers triggering the re-opening of the prepare task. The Platform facilitates multiple review tasks.	Noted
7.11	Are the restrictions on more than one User working on the same "Compliance Instance" (for a single Firm) at the same time?	No restriction on User working on an instance at the same time. Each question (node) is fully audited and time-stamped. Where two users access a single question at the same time only one Users can edit that question. Users are notified where their answer has not been recorded and they will see the other Users answer that has been recorded.	Confirmed
7.12	Are there restrictions on more than one User working on multiple "Compliance Instances" (for different Firms) at the same time?	The FinReg Technology Platform is accessed through an internet browser. A User can utilise multiple browser tabs (multiple concurrent sessions) to access multiple compliance instances, however each session can only relate to a single organisation.	Confirmed
7.13	Can a User of the system have multiple windows open at the same time on a single "Compliance Instance"?	The FinReg Technology Platform is accessed through an internet browser. Where a user access's multiple browser tabs (multiple concurrent sessions) however each session can only relate to a single organisation.	Confirmed
7.14	Does the system allow a User to use multiple devices to support mobile working, e.g. a workstation and/or a tablet?	Yes, although the Platform has not been tailored to be used with touch screen or viewable on a tablet.	Confirmed
7.15	Does the system provide a facility for auto-saving entries made into the system (e.g. answers to questions) during a User's editing session? If so: - Can the frequency of these auto-saves be manually set? - Can the User initiate a save manually? - Can a User roll back to a previous saved version?	All activities (write, update, delete) at a Node level are saved and audited every time an activity is completed by a User.	Noted
7.16	Can the system work in an "offline" mode, with transactions transferred to the service once Internet connectivity is available and enabled? i.e. can information be completed off-line and uploaded?	Access to the platform is not possible without an internet connection	Confirmed
7.17	Does the system make use of global lists, e.g. Postcodes, risk types, ? - If so, specify what is provided.	Any pre-defined information will be included as part of the Product design if applicable. These pre-defined lists do not connect to lists outside of the Platform.	Noted
7.18	Does the system have an audit trail that includes details of all changes to: - Standing data (global lists)? - Libraries of Objectives and Risks? - All manual entries/changes to inputs made by a User?	All changes made by the user are fully audited. Changes made to the Product itself are audited and available to FinReg.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.19	Does the software directly integrate with on-line software/services? If yes, please list the packages/services in the categories below and explain the method of integration (e.g. dedicated connector, webservices, API, etc): - Companies House (for valid Company lookup)? - HMRC ? - Accounting software? - Others, please specify?	The FinReg Technology Platform can be tailored to access and facilitate API integration. The ISQM 1 solution does not include any off-the-shelf API integrations.	Noted
Firm setup			
7.20	Does the system provide for the setup and maintenance of a Firm's entity setup, including: - Name and type of the firm (Company, Partnership, etc? - Address and contact details? - Company registration information? -- Business structure and model? - Details of the ownership/management of the firm? - Associated Professional/Legal/Regulatory bodies?	The Product includes an entity and environment section to allow Firms document the nature, scale and circumstances of the Firm including key information relating to the Firm. All items listed are available for documentation.	Confirmed
7.21	Does the system allow the entry of supplementary information? If yes, can this be uploaded and held against the Firm?	Additional data points can be added with data capture supported in different locations throughout the Product through data upload.	Noted
7.22	Does the system allow Firms to be linked? If yes: - Can the system automatically copy information from an associated Firm's record when required? - Can this be manually overridden?	N/A	Compliance for firms will likely be separate.
7.23	Does the system allow all "Compliance Instances" created for a Firm to be: - Shown as a list on-screen? - The details viewed on-screen? - Details to be printed out?	All Instances can be viewed on screen in a single view on the basis that they are in the same Organisation and the User has access to the relevant Instances. All information captured is reportable.	Confirmed
7.24	Can the services undertaken by the Firm be selected from a master-list so as to define the areas of operation (and thus operational risk) of the firm?	Within the Entity and Environment section on QMCore, a Firm can document the specific characteristics of the Firm that are required to be considered in relation to ISQM 1. Included in this section is the type of clients and services that the Firm provide. QMCore includes indicative services as part of this section.	Noted
7.25	Can the selected services be amended if the Firm changes what it offers to it clients? If so, is a dated history maintained of the services selected ?	All responses can be amended at any time with an audit trail maintained of all changes completed.	Confirmed
7.26	Can document files be uploaded against a client [to support the Risk Assessment]? - If yes, what format of files is supported, e.g. PDF?	Document files can be uploaded at specific points in sections of QMCore to support the responses provided. There is no restriction on the type of files that can be uploaded from images through to word, PowerPoint, excel, text files and PDFs, although zip files should not be uploaded.	Confirmed
7.27	If documents can be held against clients, does the system have functionality to manage these documents, including the ability to: - Upload/download documents? - Mark documents as reviewed and/or approved? - Manage document retention (for GDPR compliance)? - Other, please specify?	Documents can be uploaded and downloaded by Users and document reviews are completed through the tasks associated with the document or through the comments in the audit trail.	Confirmed, but this is not a comprehensive document management system.
Regulatory risk assessment libraries			
7.28	Does the system contain a series of libraries of Risk Assessment components/objectives that cover different regulatory requirements, e.g. ISQM? If so please list the regulatory requirements covered.	QMCore covers the requirements of ISQM 1. As part of QMCore the Risk Assessment section includes pre-defined Mandatory Objectives and Specified Responses as set out in ISQM 1. Additionally QMCore includes a risk library that Firms can leverage as part of the completion of their Risk Assessment.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.29	Can a Risk Assessment type be selected based on the type of Firm identified during its setup? If so, is the type of the associated Risk Assessment selected automatically by the system based on the details entered previously?	QMCore includes some configurations based on inputs selected at the outset of the assessment. As part of the Risk Assessment a Firm can access all their objectives, risks and components and select the relevant items for their Firm based on the nature scale and complexity of the Firm.	Noted; limited. E.g. If part of a network the network questions would be enabled.
7.30	Do the Risk Assessments provided cover all the areas of work selectable during the Firm setup process as above?	QMCore includes some configurations based on inputs selected at the outset of the assessment. As part of the Risk Assessment a Firm can access all objectives, risks and components and select the relevant items for their Firm based on the nature scale and complexity of the Firm.	Noted
7.31	Does a library contain: - A series of sections/headings (i.e. Components) that match those in the associated regulatory requirements? - A set of sub-headings (i.e. objectives) that match the next level in the regulations selected? - A Risk Assessment containing a series of pre-defined risks grouped under the headings and sub-headings? - Input forms for the collection of associated data required by the system? - Other settings, please specify?	Libraries include data based on: - information and data points captured on the platform that are detailed in ISQM 1; and - Indicative risks based on the risk library. The libraries are read/write or rea- only depending on their source. The Risk Assessment section includes data entry points which the Firm enter based on the characteristics of their Firm to allow for the tailoring of the risk assessment to be specific to the Firm in question.	Confirmed
7.32	Do all the Risks have additional guidance and useful links should further clarification be required by the user?	Within the Risk Assessment the ISQM 1 standard is available for Users to access. References are included for objectives and responses to aid review of the standard.	Confirmed. A button next to the tool-tip can be selected.
7.33	Can risks be set as mandatory by the system? If so: - Can non-mandatory risks be set as mandatory by a User in the Firm with appropriate permissions? - If so, can they then be reset to be optional?	In line with ISQM 1 there is no concept of mandatory risks, risks are based on a Firms risk assessment of their Organisation.	Noted. The Standard doesn't set risks, it's up to the firm to identify and assess them.
7.34	Can Risks be set to different levels of (i) possible impact and (ii) likelihood by the system? If so: - Please detail the levels provided. - Can these be set/amended manually by a User? - How are impact and likelihood combined to identify "high risk" items?	The Risk Assessment includes the ability to rate risks based on likelihood and impact. Each criteria can be rated based on high, medium and low with an output being calculated to ascertain if the risk is a Quality Risk. All pre-populated assessments can be manually overridden.	Confirmed
7.35	Does the system contain a series of possible responses to each of the various risks in the library? If so: - Does this apply to all the risks or just some? - Can these be marked as mandatory, i.e. one of the possible responses must be selected as opposed to allowing an [alternative] entry to be made by the User?	QMCore contains specified responses as set out in ISQM 1. QMCore allows for the User to define the additional responses that the Firm has in place to mitigate the risks identified.	Noted. Only the responses in the Standard are included.
7.36	Are suggested risk mitigation / remediation steps included against each question?	All mitigation / remediation are defined by the User.	Noted, set by the user.
7.37	Does the system provide notes of the steps that could be taken to address each of the high risk outcomes?	All mitigation / remediation are defined by the User.	Noted, set by the user.
7.38	Can Risks in the Library be linked? If so, explain how this operates.	Risks can be linked to both objectives and responses. Multiple responses can be linked to each risk and each risk can be subsequently linked to multiple objectives. Once a risk has been linked to a response this linkage is applied to all uses of the risk.	Noted
7.39	Does the system provide the option for an authorised user in the Firm to manually amend a Risk Assessment Library?	Once a risk has been added to the Risk Assessment Users with read/write access can edit and amend the risk as appropriate. All changes are captured in the audit log. Additionally Users can add User defined risks.	Confirmed
7.40	If so, is there the ability to: - Add in new sections, sub-sections and risks into a Library? - Supress parts of the Library structure (and thus the associated Risks)?	Where a risk is not added to the Risk Assessment it remains in the User selection dropdown as an option but is not included in the risk assessment dashboards. Users can define risks as required.	Noted
7.41	Can a new Library be created based on an existing Library, then manually amended?	No. Can roll forward within an organisation but not copy between organisations.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.42	Can the inbuilt question hierarchy in a Library enable/disable [expose] specific risk questions in the Library depending on answers provided by Users to questions in another section of the Library?	There are inbuilt workflows within the product itself and within the libraries.	Noted
7.43	If so, can the amended library be saved as: - The new default library? - A future-selectable library? - Other, please specify?	See 7.41 above	Noted
The Firm's risk assessment			
7.44	Does the system allow one or more instances to be selected as active for the Firm? If so, is the associated Risk Assessment then made available for editing by Users?	QMCore is a system of quality management solution that is maintained on an on-going basis. As such Firms would only have a single instance active at any point in time	Noted
7.45	Can a "Compliance Instance" be marked with a status, for example: - "In Progress" for the current "Compliance Instance"? - "Complete" for a closed or historic "Compliance Instance"? - "Locked" for an archived "Compliance Instance" - Other, please specify?	Each Instance can be noted as "In Progress", "Complete" or "Locked". All instances are in the "In Progress" state until all Tasks associated with the Instance have been completed. This automatically moves the instance state to "Complete. Once an Instance is complete, it can be "Locked". Once an Instance is "Locked" all tasks are hidden and the instance is in a view only mode for all Users who previously had access.	Confirmed
7.46	For each of the Risks in the instance can each Risk Assessment item be: - Assigned a date, status (code), and priority? - Be assigned to a specific User or Users to address the Risk? - To another User to review the answer(s) provided? - Can Actions be allocated that can be assigned to specific Users, dated and tracked?	Risks in the Risk Assessment can be configured to: 1. All fall under a single task; or 2. Fall under separate tasks. Tasks allows for the assignment of due dates, status of completion and priorities. The Platform includes the ability to create Delegate Tasks. Elements of any task can be delegated to other Users which creates a new task for the User to complete. Risk can then be sent for Review under a Review Task which can be configured as noted above in 7.45.	Confirmed
7.47	Can a User change the status of an Action so that it can be tracked? If so are the following status supported: - Not started? - In progress? - Completed? - Reassigned [to another User]? - Other, please specify?	All "Actions" are referred to as "Tasks" on the Platform. The state of each task can be changed by a user unless there is a logical exclusion. Some logical exclusions include: Task state cannot be moved from "In Progress" to "Not Started" when responses have been added; and Task state cannot be moved to "Complete" unless all "Mandatory" responses have been included or delegated tasks related to the main task have been completed.	Confirmed. Status indicators are colour coded for ease of use.
7.48	Does the system provide an easy way for the User to navigate the Risk Assessment and make entries against each of the risks?	Users can assess the risk assessment in a number of ways including: - Risk Assessment Dashboards click through (see dashboards below); - Risk Assessment Of Quality Objectives table; and - Objectives, Risks and Responses tables. Each table includes a clickthrough within the screen opening as a "pop up" on the screen allowing the User to close the pop up to return to the table. Tables include filtering dropdowns with search features for ease of use.	Confirmed
7.49	Is it possible for a User to expand and collapse sections of the Library to simplify navigation?	Tables include row grouping where multiple rows exist.	Confirmed

Ref	Requirement	Vendor Response	Reviewer Comments
7.50	Does the system have search functionality to enable the user to jump to a specific question?	Each column is searchable and can be filtered with multiple filters being in place at the same time.	Confirmed
7.51	Against a Risk, can a User enter: - A selection from the predefined list (if appropriate)? - A free-text response/description? - A change to the Risk's severity? - A potential mitigation / remediation? - Other, please specify?	The risk assessment includes the following information across each Risk: - Risk Name - SOQM Reference - Risk description - Risk Impact & Impact description - Risk Likelihood & likelihood description - Evaluation Outcome - Risk Assessment Override - Quality Risk response override	Noted
7.52	Can a User upload a document against a Risk, that might be used to provide supporting evidence for a mitigation / remediation?	Document Uploads against risks can be added through a configuration request.	Confirmed
7.53	Is a comments box available under each question, to provide the facility to capture additional information relevant to the Risk or its mitigation / remediation?	Description boxes are available as noted at 7.51 above. Comments can be added to any response and are included in the audit trail.	Confirmed. Free text can be added.
7.54	Can a user update an Action: - Changing it's status? - Assigning the action to another User? - Adding a diarised reminder? - Upload a document against it? - Change it's due date? - Other, please specify?	Tasks can be manged and updated as noted at 7.46 above. Additionally the Platform allows Users to create actions based on "External Tasks". An External Task can be added when an action not connected to responding to a question is required (e.g. an external task to check a policy etc.). External Tasks include the following characteristics: - State of Completion - Assignee - Owner - Comments - Document Upload - Due Date - Priority Reminder system functionality is under development.	Noted
7.55	When a User is the senior responsible person in the system, can notifications be sent automatically to that User when there is an update on an action assigned to them or a members of their team? If yes, how is this achieved?	Responsibility & Access to edit data in a Product is via the "Task" associated with the Node. All Tasks include email notifications which are sent notifying the User that an action has been completed relating to that Task. Actions relating to the Task include: - Task Status being changed - Task Priority being changed - Due Date being added / changed - Comments being added to the Task. Changing of the status of a Task is an indication that the work has been completed (see 7.47 above).	Noted. Review of risks can be delegated to the senior responsioble person; however as every risk is available for review by other team members (as required by the standard) delegation is a manual exercise by users.
7.56	As well as allowing any member of staff to update actions assigned to them, does the system enable this to be done by a central compliance team?	All Tasks have two user groups assigned to them: - Owner / Creator User Group - This is an administrative role that can be assigned to multiple users; and - Assignee / Preparer User Group - This is based on predefined user groups and / or individuals. Roles / Groups are managed by the Customer at all stages with access to manage access and users.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.57	Does the system show progress through the Risk Assessment: which sections have been started and which completed?	As noted above the tasks within the risk assessment demonstrate progress. As noted below, the Risk Assessment Dashboard also demonstrates counts and totals of objectives, risks and responses added throughout the process.	Confirmed
7.58	Does the system allow subsequent amendment of individual entries, without the need to walkthrough complete sections of questions again?	Individual entries can be edited once a task is in the "In Progress" state. Where a review was completed (or is required) recompleting/editing a node will trigger a re-review.	Noted
7.59	Is a summary provided of the number of questions answered and the number falling into each risk category? If yes, is there drill through to the underlying questions?	Risks (and the total number of risks) can be reported within the dashboard reporting. Categorisation of risks by risk evaluation outcome (based on impact and likelihood) is available. All risks can be categorised by component. All dashboards contain drill down capability (where applicable)	Confirmed
7.60	Does the system allow a compliance manager to track overall progress of a project to achieve compliance with a SOQM against a baselined status? If so, how would this be undertaken?	Progress within a SOQM may require management in multiple ways including: - Status of open/in progress tasks associated with any/all elements of the SOQM; - Number of responses monitored; - Number of deficiencies/remediation items; - Status of Review of Remediations. All of the above can be tracked via tasks and dashboard reporting.	Noted
7.61	Does the system log the completion of the various sections of the input forms once all questions in a section have been completed?	As all activities are managed by tasks the status of tasks (on screen via icons or via the task screen) indicate the status of the completion of inputs.	Confirmed
7.62	Is it possible to manually log a section as complete even if an answer/information has not been provided for every question in a section?	Tasks can be completed once all mandatory items have been completed.	Noted
7.63	Can a completed section be manually marked as not completed?	Task states are not started, in progress and complete.	Noted. Reviewed tasks might be rejected.
Monitoring			
7.64	Does the platform provide functionality to enable the Firm to monitor its current Risk Assessment on an ongoing basis and track monitoring and mitigation / remediation events? If so: - Can the a set of monitoring activities be defined and dated? - If it is decided that monitoring of a risk is not needed does the system allow this to be identified and the rationale/reason for this to be logged?	QMCore allows Users to assess and document at a response level (within the risk assessment) responses which will be subject to monitoring activities. Where a response is not being monitored then this can be documented. For responses which will be monitored a monitoring workspace can be set up to capture the key information related to the monitoring and upload evidence of the monitoring completed.	Confirmed

Ref	Requirement	Vendor Response	Reviewer Comments
7.65	Does the system provide an inbuilt list of statuses of monitoring activities, including: - Effective - Partly effective? - Not effective / deficiency? - In progress? - Unanswered? - Others, please specify?	Each monitoring activity has a task status noting if the monitoring is "Not started", "In Progress" or "Complete". In line with the requirements of the standard, key outcomes can be captured by Users through adding "Events" in the Event Log. Events include: Monitoring, Deficiency Review & Remediation, Actions and Observations. - Monitoring events allows the Users to summarise the notes related to the monitoring; - Deficiency Review & Remediation allows the Users to document the notes and reference work done related to identifying a deficiency in the monitoring workspace, and the remediation to be completed. Each Deficiency and remediation is then sent for remediation action review with a status assigned to the outcome of the process being "Satisfactory", "Unsatisfactory", and "In Progress". Observations allow users to capture any other items arising from the Monitoring including: - Findings - minor; - Findings - positive outcomes; - Findings - continual improvements; - Other Observations; or - Communication of Event Outcomes.	Noted
7.66	If so: - Are other statuses included? - Can the User add/amend/delete statuses?	See above.	As above
7.67	Can monitoring information be entered and tracked against each risk/response, including: - Monitoring User? - Monitoring completion date? - Monitoring next due date? - Monitoring result, selected from the list of status (above)? - Current mitigation / remediation status? - Assigned User?	Monitoring Users can be assigned the Monitoring workspace task which includes user information, completion date and due dates. The tasks includes the status above. Event log entries allows for the capturing of statuses as noted above.	Noted
7.68	Can a User upload a document against a Risk, that might be used to provide supporting evidence that monitoring has been undertaken and/or that mitigation / remediation has taken place? E.g. a testing template.	Each Monitoring workspace allows for the upload of supporting documentation connected directly to the relevant response.	Confirmed
Dashboard			
7.69	Does the system incorporate dashboard functionality such that the current status of a Risk Assessment and associated actions can be presented to the User on a single screen?	QMCore includes dashboards related to the Risk Assessment, Monitoring & Remediation workspaces and the Event Log. All dashboards are configurable per instance.	Confirmed
7.70	Can a set of dashboards be presented to the User on their "home screen" when they login to the system?	The Users "home screen" is their task screen. This screen provides a listing of all tasks which is user is part of. This screen includes a simple dashboards showing tasks by state, tasks by priority and a table of instances by product.	Confirmed
7.71	Are there dashboards showing: - Totals of Headings (Component), Sub-headings (objectives) and Risks? - Progress of any section/sub-section, i.e. Risks by status? - Progress of individual Risks? - Risk totals by severity and/or status? - Whether there are outstanding Actions? - Action totals by status? - Whether there are associated documents logged in the system? - Other, please detail?	The Risk Assessment dashboard includes several indicative graphs including inter alia, counts of objectives, risks and responses, count of risks by component, objective by total risks, weighting of risk, quality and non quality risks, response documentation risk by responses and response owners. All dashboards are based on an underlying data set including: Component, objective, risk name, risk weighting, quality risk, response name, response document upload, response owner. Additional data fields captured can be added to the underlying data set based on a configuration request.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.72	Can the User navigate directly from a dashboard into: - A currently open Risk? - Any outstanding Action? - Other, please specify?	Each dashboard graph can be "double" clicked to access the underlying data. The underlying data includes the ability to "click through" to the source data entry point.	Confirmed
7.73	Are dashboards automatically personalised according to the User's role and areas of responsibility under the operating compliance standard ("Instance")? If so, how does this operate?	Access to dashboards is based on access to all dashboards. The dashboards access is limited to individuals who require access (e.g. individual completing the risk assessment, individuals with operational responsibility and ultimate responsibility etc.). Dashboard access can be limited to viewer access.	Noted
7.74	Is possible to set alerts/reminders/appointments from the dashboard, e.g. To regularly review a "Compliance Instance"?	Currently the functionality to schedule future dated tasks is in development.	Noted
7.75	If so, do these integrate with Microsoft Outlook?	All task on the system generate an email to a User notifying them that they have an open task or a task has been updated for them.	Noted
7.76	Can a User create a custom dashboard?	Dashboards can be configured by users in the base QMCore product. Additional dashboards can be added by configuration requests as required.	Noted
Reports			
7.77	Does the system provide a series of inbuilt reports that cover: - The details of a client risk assessment? - Individual sections of an assessment, and the underlying questions and answers? - Lists of policies - Client details - Training reports - Other, describe the reports available.	The product includes a number of reporting functions and features including: - Risk Assessment Dashboard - Response M&R Dashboard - Event Log Dashboard. Each dashboard is configurable with indicative initial graphs which can be tailored or amended by the users. Excel dumps, PDF reports of dashboards and word reports are available for all data.	Noted. See also 4.30
7.78	Does the system provide a series of inbuilt reports that cover the monitoring activities and ongoing progress of this?	The product includes a number of reporting functions and features including: - Risk Assessment Dashboard - Response M&R Dashboard - Event Log Dashboard. Each dashboard is configurable with indicative initial graphs which can be tailored or amended by the users. Excel dumps, PDF reports of dashboards and word reports are available for all data.	Noted. See also 4.30
7.79	Does the system provide the ability to export/print a summary of the status of the quality system being monitored (the "Instance"), e.g. for provision to a Regulator?	The product includes a number of reporting functions and features including: - Risk Assessment Dashboard - Response M&R Dashboard - Event Log Dashboard. Each dashboard is configurable with indicative initial graphs which can be tailored or amended by the users. Excel dumps, PDF reports of dashboards and word reports are available for all data.	Confirmed
7.80	Does the system allow drill through from a report into the underlying Assessment section/question?	All dashboards include the ability to filer across the dashboard and to drill down and interrogate the underlying data. Data drill down is also clickable to access the input screens.	Confirmed
7.81	Are all reports adequately titled and dated? e.g. report name, Firm name, pages, numbers etc.	Reports include the name of the instance and (where applicable) page numbers. Excel documents are named based on the report name and the time and date created. Details on the instance can be added.	Confirmed
7.82	Do the reports provide totals where applicable?	Yes, where applicable. QMCore dashboards can have totals configured as required. PDF reports of graphics includes summary tables. Excel dumps are data dumps and no totals are included.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.83	Does the system allow the layout of reports to be customised: - Font? - Paragraph style? - Page format? - Watermark, e.g. "Draft"? - Company logo/graphic? - Other, please specify	Word based reporting templates are provided which can be amended and formatted with assistance / training. See above re dashboard configuration.	Noted. See also 4.30
7.84	If so, does the system allow graphics and/or the Firm's logos to be incorporated in the page formatting?	Logos and graphics are possible to be added to Word based reports.	Confirmed
7.85	Can all reports be print previewed?	Reports are automatically generated with no restriction on the time to run.	Noted. See also 4.30
7.86	Does the reporting functionality have the facility to scroll up and down when output to screen?	Reporting functionality utilises PDF, Word and excel. On this basis all outputs have the same functionality as the output medium.	Noted. Auto-downloads ready to open and print.
7.87	Can reports be output directly to other formats e.g. Excel, CSV, txt, XML, PDF etc. for any period of time required? - If so, please state the formats supported.	Reporting formats includes PDF, word and excel.	Confirmed
7.88	Is it clear when a document or report has ended (e.g. totals or end markers)?	N/A - see reporting mediums above.	-
7.89	Is a report writer provided as part of the software?	Word based reports can be configured by Users. Users can receive additional training to configure reports or request report configuration.	Noted. See also 4.30
7.90	If so, please provide details of: - The level of knowledge required to use it (beginner, user, expert). - The level of customisation provided.	Word based reporting requires some User training for simple configuration (moving items around on pages etc. requires minimal training). More advanced training is required to bring in new data elements or add new tabular analysis etc.	Noted