


Ref			
	HEADER		
	ICAEW Technical Accreditation Scheme "Anti Money Laundering" Software Evaluation		
			
	Date completed: 24th November 2022		
	© ICAEW. Technical Accreditation Questionnaire v Y928		
	CONTENTS		
1	Introduction and Prologue		
2	Issues identified and evaluation conclusion -- <i>GLOBAL REQUIREMENTS</i> :		
3	Access and Security		
4	Data processing and reporting		
5	Usability		
6	Hosted and SaaS operation (if applicable) -- <i>SPECIFIC REQUIREMENTS</i> :		
7	Anti Money Laundering		

Ref		Vendor Comments	
1.	<u>INTRODUCTION AND PROLOGUE</u>		
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: <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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. <p>It is essential, when software is implemented, for appropriate support and training to be available.</p>		
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			
1.08	General Overview:	First AML streamlines the entire anti-money laundering onboarding and compliance process for accountants. Its platform allows accountants to onboard individuals, international and complex entities easily, making an otherwise complicated and manual onboarding process simple for end users and cost effective and compliant for firms.	
1.09	Supplier background:	First AML was founded in New Zealand in 2017, and has since expanded into Australia and the United Kingdom. It has more than 165 employees globally, 500+ customers and over 375,000 pre-verified entities in its network.	

Ref		Vendor Comments	
1.10	Product background and suitability for the user:	First AML identifies the ultimate beneficial owners (UBOs) for complex entities and ownership structures, as well as collecting and verifying required identity documents and company documentation to ensure compliance teams have all the data they need to make informed risk based decisions. First AML also conduct all PEP, Sanctions and Adverse Media screening on an ongoing basis. In essence First AML removes their administrative burden, giving clients the freedom to maximise their operational efficiencies while keeping their risk in-house and meeting AML compliance requirements.	
1.11	Add-on modules:	N/A	
1.12	Typical implementation [size]:	First AML is best suited for firms who onboard at least 5 customers a month and who transact primarily with corporate or international entities.	
1.13	Vertical applications:	Not required when related specifically to client onboarding.	
1.14	Server platform and database:	First AML uses AWS cloud services. Our clients are not required to have additional servers or databases	
1.15	Client specification required:	First AML creates the Firm Account and adds all relevant users during implementation. First AML can be used with all modern browsers using desktop, tablet and mobile devices subject to the practicality of the screen-size of the device	
1.16	Partner network:	We have an active partner network including Alliance, Referral and Integration partners.	

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)		
	* Users cannot create saved searches /filters; but items can be easily/quickly selected from the dashboard..		4.36
	* Reports cannot be added to user menus and user-defined reports cannot be created and saved.		4.35 4.37
	* Limited customisable branding is supported.		5.02
	* It is not possible to store preferences and default values on a per-user basis.		5.09, 5.16
	* The system does not allow the definition of user-defined fields, layouts and forms.		5.10, 5.13
	* The user manual/help is not editable by the end-user. There is no traditional 'manual', but rather an on-line Help Centre containing articles and help information.		5.22, 7.50
	* ESCROW is not provided. Note that this is not unusual for this sort of software [subscription] service.		5.23
	* Service credits are not provided should the system be unavailable.		5.33
	* No current links between the software and other packages inc links to spreadsheets. This is not required. There is a .CSV import function via an excel spreadsheet template to upload bulk client information. In addition a comprehensive set of APIs are available.		5.41, 5.42 5.46
	* The supplier has a test environment but this is not offered to users to test software changes.		6.14 6.62-6.64
	* No SLA is provided relating to service availability.		6.28
	* No ability for customer to specify or take their own backups.		6.51
	* Only English is currently supported.		7.04
	* The FirstAML platform does not provide risk assessments; its focus is to provide "AML On-Boarding" (KYC/CDD).		7.20, 7.21 7.32
	* The platform does not provide AML training.		7.35-7.39
	* The platform does not provide AML policy templates or AML risk assessments.		7.41-7.65 7.71-7.98
	* The platform does provide functionality to allow internal referral of a client to the firm's MRLO.		7.122
	* The user (Accountant) is not able to share a dashboards with their client.		7.125
Evaluation conclusion			
2.03	For the specific use-cases in support of accountancy firms complying with their AML Client On-Boarding (KYC/CDD) obligations it is a solid and capable solution. It continues to be actively developed and enhanced. Members should be aware of the considerations listed above, and fully understand the role that it can play in an engagement. * 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 *		
2.03	Note that FirstAML make it clear that their platform's focus is to provide assistance with AML On-Boarding as opposed to AML-related risk assessments. Note that the organisation using the software will be responsible for ensuring that the way in which the software is configured and the processes defined around its use are in line with local legislation.		

Ref			
Disclaimers			
2.04	<p>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.</p>		

Ref	Requirement	Vendor Response	Reviewer Comments
3.	<u>ACCESS AND SECURITY</u>		
Access control			
3.01	What security features are included to control access to the application?	<ul style="list-style-type: none"> - Username and password authentication with complex password requirements. - Ability to integrate product into a customers existing user directory (SSO) which allows them employ MFA or other controls as supported by their user directory. - Use of an industry-leading IDaaS product to implementat Authentication (Auth0) which includes additional mechanisms to identify compromised passwords, brute force protection etc. - Role-based per-customer and per-office access control to product. - Scope-based and per-customer access control to the Public API. - For Customers without their own internal SSO service, additional MFA options and Social login support (google,apple,microsoft) login options are being released in next 2 quarters. 	<p>Username/password access confirmed.</p> <p>Noted re MFA and IDaaS.</p> <p>Public API is described in detail (with examples) for potential developers. See 3.07 below.</p>
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?	<ul style="list-style-type: none"> - Yes - access to functionality is controlled through a set of capabilities (fine grained permissions). The capabilities are assigned in sets to roles, and those roles are then assigned to users. - The individual capabilities assigned to each role are utilised to control the ability to see functionality available (menus and links) - In addition our product has functionality to restrict access for a user to a subset of offices within an organisation (all AML cases created in our product are related to an office) allow access to be further segregated. 	Confirmed. Multiple pre-built roles are provided.
3.03	Is this access to the application managed by:- - Individual user profiles? - User groups or job roles?	<ul style="list-style-type: none"> - Access is managed on an individual user basis through the ability to assign users a role at the organisation or office level <p>Suggested wording:</p> <ul style="list-style-type: none"> - Clients of First AML can internally manage their employee's access to our Software Platform through an administrative page or portal which allows authorised staff members from your Company to add or remove users, and assign them to specific offices. Permissions are granted on a role basis 	Confirmed
3.04	Can a report be produced detailing all current users, their user groups if relevant, and their authority levels and/or access rights?	<ul style="list-style-type: none"> - Yes this report can be produced by request to our customer success team as a spreadsheet, or the list of users with assigned roles can be easily seen in our UI as well. 	Noted
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?	<ul style="list-style-type: none"> - We do not have the ability for customers to tailor or customise the list of available menu options in our product but we can confirm that visibility of menu options is controlled by the capabilities assigned to the current users role. - Additionally, some menu options are displayed or hidden based on the pricing tier / plan a customer is on in our product (higher pricing tiers can unlock additional features/options). 	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?	- Our security implementation does allow for the separation of read vs. write, with an example of a read-only role being our "Auditor" role which is generally assigned to external auditors undertaking an AML audit of a customer. - Due to the nature of our product being a system of record for AML legislation for our customers, each AML case has a status, and based on the status some operations may not be available to certain roles, to ensure no accidental editing could be done to a completed AML case (which could remove evidence required for an AML audit.	Confirmed. Some roles are read-only.
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?	- Our platform is a SaaS product, and we don't currently expose it in a way that an external report writer or database connection could directly interface with it (such as ODBC). - We do however provide a Public API that customers can integrate against, as well as approved 3rd parties, which allows for the development of software that integrates with the information held within our platform. Details can be found here: https://firstaml.notion.site/First-AML-Public-API-535d640d711b48359b3e49005e642063 . - The user access security controls are not applied in quite the same manner as our signed in users, as the restrictions applied to our user roles would hinder the development of common integrations. We do however secure all access to the API utilise a mechanism called OpenID, and these API clients have their capabilities restricted by a set of scopes. - Both our Public API and our main product undergo quarterly external security penetration testing to ensure these mechanisms are safe and secure.	Noted
3.08	Does the system security integrate with Microsoft's Active Directory or other tools that provide a single sign-on?	- Yes, we integrate with a wide variety of user directories including Microsoft Active Directory. The list of supported directories / enterprise identity providers can be found here: https://auth0.com/docs/authenticate/identity-providers/enterprise-identity-providers .	Noted
3.09	Does the system provide multi-factor authentication (MFA)?	- Currently we support MFA through the integration with a user directory such as Microsoft Azure AD or Okta (SSO). - We have plans to release Additional MFA options and Social login support (google,apple,microsoft) login options being released in next 2 quarters.	Noted
Passwords and access logs			
3.10	Is access to the software controlled by password?	Yes - with strong password complexity controls, and a range of other protections in place to prevent user of known compromised passwords, and to protect against common attacks like password brute forcing.	Confirmed
3.11	Does each user have a separate log on (user id)?	Yes - the user ID is mapped to their email address.	Confirmed
3.12	If there is no password facility please state how confidentiality and accessibility control is maintained within the software?	N/A - customers must login to access the system.	-
3.13	Are passwords masked for any user logging in?	Yes - passwords are one-way hashed and stored in our industry leading IDaaS Auth0. There is no way to retrieve a clear-text version of the password.	Confirmed
3.14	Is password complexity available and enforced?	Yes - complexity is managed by the IDaaS and enforced.	Noted
3.15	Are passwords encrypted?	Yes - passwords are securely one-way hashed to industry accepted levels.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
3.16	<p>Are users automatically logged off after a pre-set idle time?</p> <ul style="list-style-type: none"> - Can the time period be changed? - Can any information be viewed without being logged in, including after logging off, if so what information? 	<p>Yes:</p> <ul style="list-style-type: none"> - Users are automatically logged off after a pre-set idle time. - Currently the time period is not customer configurable. - Other factors (such as change of a devices location/country/IP address) will also cause a user to need to reauthenticate as a security precaution. - No information can be viewed in a logged out state. Customers must login before they can view any information. - End user forms for individuals to populate information with (such as their drivers license, passport etc.) are "write-only" as well. You can upload information, but you can not view previously uploaded information, which is by design. 	Noted
Deletion of transactions			
3.17	Is it possible to delete a transaction?	<ul style="list-style-type: none"> - Yes in some cases prior to the data being submitted, end users can delete information. Otherwise, First AML can process data deletion requests received by email. 	Noted
3.18	If so, then how are deletions controlled by the system?	<ul style="list-style-type: none"> - It is possible to mark a record as deleted in our system - but only at certain points. Our AML cases have a status, prior to a case being submitted (moving to the in-progress state) it is possible for a user to delete the record. But once an AML case is in progress, it can only be marked as abandoned, but not outright deleted by the user. This is both because it at that point is a billable event in our product, but also because it's potentially relevant to an AML audit e.g. if the case was progressed then abandoned because it was discovered an individual was under sanctions, this is still an important record to retain for a future AML audit. - We also have a rigorous process in place where First AML can undertake data deletion with a customers authorization, if an individual being verified wishes to exercise their legal rights under relevant privacy legislation (this is managed outside of our products user interface currently). 	Noted
3.19	Are deleted transactions retained in the audit trail (see below) and denoted as such?	<p>Yes, our product has a detailed audit trail which includes recording the deletion of AML cases (and any data within the case) this audit log is captured in our products internal data store, but not exposed to customers currently. If customers wish to review the audit log we are able to provide an export upon request. If processing a privacy deletion request these audit logs are removed or redacted as needed to ensure all PII related to the privacy request has been removed.</p>	Noted
Audit trails			
3.20	Does the system have an audit trail (log) which records all changes to transactions in the system?	<p>Yes, our product has a detailed audit trail which includes recording updates to AML cases - this audit log is captured in our products internal data store, but not exposed to customers currently. If customers wish to review the audit log we are able to provide an export upon request. If processing a privacy deletion request these audit logs are removed or redacted as needed to ensure all PII related to the privacy request has been removed. we do also include a customer-visible activity log providing details of major changes in case state and communications.</p>	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
3.21	Does this log also record any system error messages and/or any security violations?	<ul style="list-style-type: none"> - Our audit log captures changes to the system over time related to the product only. - We have an extensive range of other monitoring and logging capabilities that capture error messages, security events etc. into our Security Information and Event Management (SIEM) system Sumologic, which provides centralised reporting and monitoring of errors and security events, which is monitored by our engineering and security teams actively. - Security violations and error messages and pro-actively investigated, in any cases where the error or security issue would impact one of our customers in our SaaS platform they would be notified accordingly. 	Noted. Activity log shows user, date and interaction made.
3.22	Is it possible to turn off or delete the audit trail?	- No it can not be tampered with, and is regularly backed up (every 5 minutes) as well as geographically backed up to another geographic region every hour.	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?	- Yes all data in our system is uniquely identified, both by a sequential ID, and additionally in some cases by a second globally unique key (UUID).	Noted
3.24	Are all master file changes recorded in the audit trail?	The "master file" is not totally relevant in the context of our product, but all changes to data for a customer is captured into the audit log (create/update/delete/change status, or external activities being performed such as sending an email) and this is centrally stored in our SaaS platform.	Noted
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?	<p>Yes:</p> <ul style="list-style-type: none"> - We have tools available to our privacy & security team to allow them to assist customers in fulfilling privacy requests (both requests for information and right to be forgotten) given our role as a data processor on behalf a data controller (our customer). - We work to the timeframes of global privacy legislation in servicing privacy requests to ensure our customers remain compliant with relevant privacy legislation. - Our product is designed with privacy in mind, and captures all relevant consents (and records those internally) as part of collecting data from the individuals and entities being verified. 	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
3.26	Describe your use of sub-processors if any?	<p>- First AML uses some sub-processors as part of contractual necessity and legitimate interest as detailed in our privacy policy at firstaml.com/privacy-policy. This includes cloud hosting (AWS), various data source providers for verifying individuals and entities, and other sub-processors such as cloud services, and data analysis software.</p> <p>In relation to data sources for verifying individuals and entities:</p> <ul style="list-style-type: none"> - These data sources are API layers over the top of companies such as credit bureaus. - The information passed to the data sources include PII (such as name, address, date of birth, ID document numbers and expiry dates etc.). - The information returned from these data sources will verify if a match was found or not, and against which sources. - The data sources do not store or hold the information passed to them, and only have the information passed to them for the period of time required to service the request. - We maintain a list of our data sources, and have the associated DPAs (Data processing agreements) in place with each data source, each data source also undergoes a security review as part of our ISO-27001 compliance process. 	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?	<p>No:</p> <ul style="list-style-type: none"> - We don't currently provide information to our customers about our backup and restore process in our help centre (which is the equivalent of our user manual) however data backup and recovery is handled internally by First AML utilising AWS tooling. There is more information about this below under responses 3.28/3.29. - Our ISO-27001 compliance audits also evaluate how our backup process works, including ensuring that we regularly test the restoration process as part of our overall business continuity exercises. 	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
3.28	How often are backups taken and to what point can restores be done?	<p>- We utilise 2 main storage components in our solution for data - Amazon S3 (document storage), and Amazon RDS Postgres (a database server).</p> <p>Amazon S3: - Amazon s3 creates backups of any uploaded document in near-realtime in another geographic region. - All updates to documents stored in s3 is versioned. - As such we have the ability to recover to any point in time for documents, even if we experience the lost of an entire AWS region (which is a collection of 3 or more separate data centres in a single geograhic location).</p> <p>Amazon RDS Postgres (our database server): - We have continuous backups enabled for a 35 day period, allowing point-in-time recovery (meaning we recover to any point in time within the last 35 days). - We also perform hourly snapshot backups, which are retained for at least 366 days, allowing recovery beyond a 35 day period to a granularity of the nearest hour. - Backups are replicated to a second geographic region as well, allowing recovery in case of loss of</p>	Noted
3.29	How does the software facilitate recovery procedures in the event of software failure? (E.g. roll back to the last completed transaction).	<p>The platform is hosted and managed by First AML (SaaS product) so in the case of needing to recover from failure, First AML would utilise the restoration capabilities of Amazon S3 and Amazon RDS to restore the state of the system. Depending on the situation and context, we may restore that data into a seperate instance of the database and utilise that data to repair the primary instance to ensure no loss of customer data or system availability occurs during the restoration process.</p>	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?	<p>No - our platform regularly persists changes on screen where applicable (and will reflect changes being made by other users to the same record, by polling for changes in the background).</p>	Noted
3.31	What features are available within the software to help track down processing problems?	<p>Our platform is a hosted / managed solution, so problems related to the performance of our software platform are managed internally. Customers can raise a support ticket with our customer success team if they identify an issue, and depending on the nature of the support issue our customer success, billing, engineer or security teams will handle the resolution of the problem. This is part of what our platforms monthly platform fee covers.</p>	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?	Our functionality is exposed through a rich UI that includes self-explanatory menu items and other UI elements. We make use of in-app notifications and cues to explain functionality changes over time (new feature releases).	Confirmed. Very clear and easy to navigate.
4.02	Are these menus user/role-specific?	UI element visibility is controlled based on the capabilities associated with the roles.	Confirmed
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?	Yes	Confirmed
4.04	Does the software provide input validation checks such as: - [account] code validation? - reasonableness limits? - validity checks?	The software platform validates data against a variety of formats such as dates, selections of options and formats of ID document identifiers. It does not implement reasonableness limits.	Confirmed
4.05	What control features are within the software to ensure completeness and accuracy of data input?	For AML verifications the data is input by end users and includes standard validation around data types etc. The nature of AML is that all data is verified for accuracy against data sources (credit headers, electoral role, document tampering and biometric checks etc.) which ensures that all data is verified accurate and that the individual is identified as a real person and the information they are presenting has not been tampered with and is authentic.	Noted
4.06	How does the software ensure uniqueness of the input transactions? (i.e. to avoid duplicate transactions)	All AML cases, individuals and entities are created with unique identifiers. All changes to data are executed in transactions ensuring partially complete data is not captured in the database.	Confirmed
4.07	Is data input by users validated by scripts or routines in the browser, or other client software, before transmission to the server?	Yes validation is performed client-side in the First AML UI prior to be transmitted to servers, and is then validated against server-side.	Noted
4.08	Is data input by users validated by routines running on the server before data files are updated?	Yes data is validated server-side before being stored, with validation errors return to the UI if the data is not considered valid.	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?	Yes data is validated client-side and server-side to prevent against maximum lengths and unacceptable values.	Noted
4.10	Are responses to erroneous data input clear so that they do not lead to inappropriate actions?	Yes	
4.11	Does the software have an automatic facility to correct/reverse/delete transactions?	Data is not persisted if not valid or incomplete. Data can continue to be corrected via the UI or API until the AML case status moves to complete.	Noted
4.12	If yes, are these logged in the audit trail?	Yes all changes made to the information in the system is captured in the internal audit trail.	
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?	Yes, file uploads will fail unless they are completed fully, resulting in no information being stored.	Noted
4.14	Are messages provided to users clearly explaining whether the data entry or file upload has been processed successfully or not?	Yes	Confirmed. Invalid options are greyed out, incomplete entries are flagged, and data entered in an incorrect format is flagged and the reason explained.
Import and export of data			
4.15	Can files/attachments be uploaded and stored against any transaction?	Yes - common file types e.g. pdf, jpeg, docx can be uploaded against an individual or a case (verification request).	Confirmed; there is a separate "Documents" tab to save files to the case. The user can add notes as well.
4.16	Is there an additional charge made for storage of uploaded files? - If yes, please indicate the cost.	No - this is included in our monthly platform fee.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
4.17	Can data be imported into the system from multiple types of files, e.g. XLS, text, CSV?	Yes - we currently support jpeg, pdf, docx. xls and csv file uploads are not currently supported	Noted
4.18	Explain how the system validates imports into the system and what happens to any import which fails?	When uploading a file fails then, an error message is displayed on screen.	Noted
4.19	Are imported /interfaced transactions detailed in the audit trail? [See also 3.27]	Yes all changes to data related to an AML case is captured in the audit log - regardless of if it's performed through the UI or API.	Noted
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?	Uploaded files can be exported by users with the correct permissions, and summary PDFs of a verification record can also be downloaded.	Confirmed. Bulk download to CSV option is provided.
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)?	N/A	Noted. Not a transactional system.
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?	Each AML case does support capturing an "external reference" to relate the AML case to external entity in another system. This external reference can be up to 255 characters of textual content.	Noted
4.26	How does the software guard against/warn about duplicate account numbers on set up?	N/A	Noted. Case numbers are unique.
4.27	How does the software enable the traceability [from, to and through the accounting records] of any source document or interfaced transaction?	Our Software/Service does not process any financial transactions. Events undertaken by users within our Software e.g. document uploads, logins, and information inputs are logged for forensics.	N/A
4.28	What drill down/around functionality is available within the software?	All AML case information can be viewed easily in the product and is exposed in our reporting functionality (which includes the ability to export data to CSV, for import into other tools for deeper analysis)	Noted
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)?	First AML's Software Platform has a reporting functionality which utilises a third party Sub-processor called Sisense who are ISO27001 and SOC2 type II certified.	Confirmed. A comprehensive set of filters is provided with this.
4.31	Is the report writer based on a standard SQL-type approach and is it flexible and easy to use?	First AML's reporting tool displays information based on filters which can be toggled as required.	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?	N/A	-
4.33	Is a comprehensive data dictionary provided to aid field selection?	N/A	-
4.34	Does the system provide a library of reports and templates which can be amended, saved and re-run?	Our system includes a number of standard reports, but these can not be configured by customers.	Noted
4.35	Can users create their own reports? If so, what are the controls on users doing this?	No, user's can not create their own reports.	Noted
4.36	Can users create saved searches /filters / queries?	No, we have flexible search and filter capabilities, but those search configurations can not be saved for reuse.	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?	On demand reporting is supported, batch reporting can be achieved through integrating with the First AML API (requires software development skills)	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
5.	USABILITY		
Ease of use			
5.01	Does the solution provide a multi-language user interface?	No - We don't provide our platform in any language, other than English, at present	Noted
5.02	Does the system allow for customizable branding and UI (e.g. corporate colour palate, upload company logo, etc)?	Partially: - We provide co-branding of all email communication outbound from our platform through uploading of company logos - We provide co-branding of our EIV and secure web forms through uploading of company logos - We do not currently support colour palettes for items such as buttons, though we intend to investigate this in future.	Noted
5.03	Does the system have a similar look and feel and overall and consistency between screens and modules?	Yes - We have created, and maintain, a design system and component library in order to have a consistent and repeatable look and feel across our product.	Confirmed
5.04	Is data entry easily repeated if similar to previous entry?	No - we do not currently offer a way to do repeat data entry	Noted
5.05	Does the software prevent access to a record while it is being updated?	No, we allow for concurrent access to the records by multiple users. Our platform polls for changes to the record in the background and will automatically refresh to show changes made by other users to the data being displayed, this refresh cycle is 10 seconds.	
5.06	Is there locking at file or record level?	Once a case has been set to "Completed" there is only one action that is able to be taken. That is to request additional work on all, or a part of the case. We also have permissions in place that allow only certain actions and parts of each case to be visible / editable by different user roles	Noted
5.07	Does the software allow for the running of reports whilst records are being updated?	This is highly unlikely in the context of our typical workflow. We have reporting functionality that allows customers to view all cases and filter these by status in real time (In progress, Ready for Review, Completed, etc.)	Noted
5.08	Can timestamps or user comments be added to transactions?	Yes - We have a notes field that is available in every case, plus an activity log that includes a timestamp.	Confirmed in activity log
5.09	Is there the ability to store preferences and default values on a per-user basis. e.g. department/team/user?	There is no current ability to store preferences and defaults on a per-user basis. We do control visibility and access to parts of each case, on a per user role basis	Noted
5.10	Does the system have the ability to provide user-defined fields with associated validation of data input?	We do not currently support user-defined fields.	Noted
5.11	Can the system provide users with reminders and notifications e.g. workflows?	We automatically send reminders to individuals we have requested to electronically verify and to end-users who have been requested to provide us with documents for the purpose of verification. These trigger after a period of inactivity. Notifications are sent to the Reporting Entity (our customer) when a case is ready for them to review.	Noted. Not user-definable .
5.12	If the system provides workflows, does it have functionality to substitute/delegate authorisations?	It is possible to configure the recipients of the ready for review notifications (sent when the First AML team have completed their work and are passing it back to our customer to review). It is also possible for a platform user to be "assigned" to a case. This gives them visibility of the case and the work being done to complete that case. No other configuration is currently possible.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
5.13	Is there the ability for users to define and configure layouts of letters and forms?	No - emails in our platform are a standard format. We intend to investigate possible options for supporting this in future. Data collection forms are not configurable. We intend to investigate possible options for supporting this in future.	Noted
5.14	Can users save the parameters of searches?	No - searches and reports are not able to be saved at present. We intend to investigate this in future.	Noted
5.15	Does the system have a "universal search" option, allowing a search to be undertaken over all modules of the system?	Yes - we have global search functionality that includes searching by common fields. These include (but are not limited to) case name, case reference, entity names, emails and phone numbers	Confirmed, with drill-through.
5.16	Can the system store menu option 'favourites' on a per user basis?	No - the platform "dashboard" displays cases in a different status order, based on user role. These have been ordered based on the common patterns / mental model of the users within those roles.	Noted
5.17	Can a user open multiple windows accessing the same or different modules of the system?	Yes - it is possible to have multiple browser windows, or tabs, open to visit different parts of the platform	Confirmed
5.18	Can more than one software function be performed concurrently?	If the platform is open in multiple windows, it is possible to run a report and submit a request for CDD at the same time. See 5.05	Noted
User documentation and training			
5.19	Is the manual provided as: - hard copy - on CD - by download - via a web-interface?	We provide training videos (via Loom) to all our customers and have a help centre, hosted with Freshdeck , that is our equivalent of a user manual. It contains articles and materials to help our customers use our platform, as well as information for end-users to help them complete any verification requests. All customers are provided with an onboarding plan and training to help them get started using our platform. Customised training is provided to customers on our top pricing tier. There is a direct link to the help centre from within the First AML platform.	Confirmed. Detailed descriptions and a large range of videos. An interactive chatbot is provided. There is also an option to directly submit a support ticket.
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?	The Freshdesk help centre contains search functionality, as well as screenshots and examples of how to use the platform. There is also an option to create support tickets that will go directly to our support team for assistance.	Confirmed, as above.
5.21	Is context-sensitive help available within the system?	Yes - there are tooltips and explanatory dialogue within our system to help the viewer understand what they're looking at, or what they're required to do.	Confirmed
5.22	Is the manual and/or help editable by the user (subject to the permissions matrix)?	No - all help and training related materials are created and maintained by the First AML team in-house.	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)?	N/A	Noted and not unusual for this sort of (SaaS) system.
5.24	Please detail the training options available?	All customers are provided with an onboarding plan and training to help them get started using our platform. Customised training is provided to customers on our top pricing tier. We also provide training videos (via Loom) and have a help centre, hosted with Freshdeck, that contains articles and materials to help our customers use our platform.	Noted
5.25	Who provides training: - Software House? - VAR?	Training is provided in-house	Noted
Support and maintenance			

Ref	Requirement	Vendor Response	Reviewer Comments
5.26	How is the software sold: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	Sales are direct from our in-house team. Though we do have strategic partnerships in place for referral-based business.	Noted
5.27	How is the product supported: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	Support is provided in-house	Noted
5.28	Do VARs have to go through an accreditation process?	All strategic partnerships are managed by a member of our team in-house. We do not currently use VARs	Noted
5.29	Is the software sold based upon number of named users or a number of concurrent users?	Product is not restricted by number of user licences, we operate a case volume licensing model	Noted
5.30	The supplier should detail the support cover options available, covering: - The hours provided? - Associated costs? - The global regions covered?	Support services are provided during normal business hours for NZ, Australia and the UK. The support costs are included in our monthly platform fee.	Noted
5.31	Detail the process by which customers raise support requests and how these can be viewed/managed?	Support tickets can be raised via the help centre and are managed by an in-house support team.	Noted
5.32	Please note the methods of support available: - Telephone? - Internet chat? - Remote access to customer workstation? - Other, please specify?	Support is managed via a ticketing system. Email and phone support is common. We are also introducing a chatbot to our support platform, aimed at helping to direct customers to the answers they need.	Noted
5.33	Do you offer service credits for failure to meet performance around SLA and uptime (if applicable)	We do not commit to an SLA as the collection of information is subject to cooperation from end-users. Our system is designed to expedite the collection of this information through follow ups	Noted. The timetable is very much controlled by the user and down to individuals to provide information requested.
5.34	What is your escalation path for tickets which have not been resolved within a reasonable time?	User can escalate with their Customer Success Manager, or through Customer Support.	Noted
5.35	How often are general software enhancements provided?	We operate on a continuous delivery model, delivering new product features and enhancements on an ongoing basis	Noted
5.36	Will they be given free of charge?	These are included in our monthly platform fee	Noted
5.37	How are enhancements and bug fixes provided to customers?	We operate on a continuous delivery model, delivering bug fixes and enhancements on an ongoing basis. Where these are customer-facing, we provide comms via the platform to let them know of the changes.	Noted
5.38	Is "hot line" support to assist with immediate problem solving available?	Our support team are available during NZ, AU and UK business hours. And, we have an "on-call" team that emergency issues are able to be escalated to if anything occurs outside of those hours..	Noted
5.39	If so, is there an additional cost involved?	These are included in our monthly platform fee	Noted
5.40	At what times will this support be available?	On-call support services for emergencies is available 24x7	Noted
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?	Our reporting functionality utilises a third party sub-processor called Sisense who are ISO27001 and SOC2 type II certified. Currently this functionality is limited to table-based displays, however we provide customers with download functionality so they have the ability to export data to a .csv file for manual manipulation. We intend to assess future display and reporting facilities based on customer needs and feedback. We do not provide links to other software packages at this time.	Noted
5.42	Can definable links to spreadsheets be created?	We do not support links to spreadsheets at this time	Noted. Not that sort of system.

Ref	Requirement	Vendor Response	Reviewer Comments
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.	Yes - all documents are securely stored via our AWS-hosted infrastructure. Common file types include pdf, jpeg, docx. These documents all relate to the verification of an individual or entity and can include (but are not limited to) ID documents, company extracts, biometric data (images and videos), and source of wealth/funds information.	Noted
5.44	Can documents be scanned into a secure repository?	All documents, whether provided via a secure web form or via the platform are securely stored in AWS-hosted infrastructure. This is done via document upload functionality. Scanning documents directly into our platform is not supported	Noted
5.45	Does the system provide data migration tools for transactional and master data sets (e.g. employees customers, suppliers, journals, invoices).	We do not provide automated data migration tools. These are done manually, upon request. Case-related information, including documents, is able to be downloaded by customers directly from our platform, or via our Public API	Noted
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?	We have a Public API available for our customers' use. This enables them to request AML services via this connection, mainly creating cases, receiving verification information and documentation and case status details. Customers are able to connect this with their CMS or any other platforms they might use for client management.	Noted. Detailed documentaton of this is available.
5.47	Does the system support mobile working?	Parts of our platform were specifically designed with a mobile-first approach. The remainder of our platform is being migrated to being fully mobile-friendly as an iterative process that's part of each new platform improvement we deliver.	Noted. This is key to the operation of the system.

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?	Solution is hosted in Amazon Web Services (AWS). We utilise a primary region and a second region for disaster recover, and have two primary regions - one for our UK and European customers, and a second for our Asia Pacific customers. UK/Europe: - Primary: Ireland (eu-west-1) - Secondary: Frankfurt (eu-central-1) APAC (New Zealand & Australian customers) - Primary: Sydney (ap-southeast-2) - Secondary: Oregon (us-west-2)	Noted
6.02	Does the customer get a choice of the jurisdiction in which their data resides?	Yes - based on being a UK/EU or APAC customer	Noted
6.03	What certification(s) do you or your platform operators hold relating to your data centres and your business operations?	Our business is ISO-27001 certified. AWS has a robust and broad set of compliance programs and certifications that can be found here: https://aws.amazon.com/compliance/programs/ including ISO-27001, SOC-2, C5 and G-Cloud.	Noted
6.04	Do you or your platform operator have an SSAE16 (System and Organization Controls) report available?	Yes, AWS does.	Noted
6.05	What are the physical controls over the:- - Premises? - Fileservers? - Communications equipment?	Customer data is stored in our Software Platform which is hosted on AWS Infrastructure. AWS has mature security posture including ISO27001 and SOC 2 type II certifications. Information about their physical Security practices is available on their website at https://aws.amazon.com/compliance/data-center/controls/ .	Noted
6.06	Is the space in this/these data centre(s) shared with any other companies?	AWS offers multi-tenant services using logical separation and other controls. More information on this is available here: https://docs.aws.amazon.com/whitepapers/latest/logical-separation/introduction.html .	Noted
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?	Our solution is multi-tenant, but utilises a shared datastore with co-mingled data between multiple customers, employing logical separation enforced by application logic. Application logic to keep customer data separated logically is regularly tested and verified by an automated test suite, and quarterly external application penetration tests.	Noted
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?	In relation to multi-tenancy, see the response to 6.07 above. Authorised employees of Customers of First AML can self-manage their employee access including assignment of appropriate user roles.	Noted
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?	As per 6.07 - Our solution is multi-tenant, but utilises a shared datastore with co-mingled data between multiple customers, employing logical separation enforced by application logic. Application logic to keep customer data separated logically is regularly tested and verified by an automated test suite, and quarterly external application penetration tests.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.10	How is [Internet] communication traffic monitored to identify potential problems before they happen: - From a performance perspective? - From a security standpoint?	We utilise Datadog for monitoring operations coming to, and within, our platform. This provides the ability to monitor a rising number of failures, resource constraints (CPU/memory/disk) and operations that have not completed successfully. There are a large number of performance metrics published by this platform that we report on, and provide ongoing monitoring via dashboards and alerts. From a security perspective, we utilise AWS GuardDuty which continually analyses operations within our Amazon Web Services environment, and alerts on anomalous behaviour (different access patterns, network port scans, data exfiltration etc). Alerts from this service are sent to the Security and Site Reliability Teams to triage and resolve.	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?	All operations that require state changes in our backend (ie data changes, updates etc) are performed by utilising queue based events. Events are placed into queues, acted upon to modify the data, and then the message removed from the queue. Failed attempts are retried automatically, and can be retried at a later date if still not successful. Database operations are wrapped in transactions to ensure that either all operations complete or none of them. This prevents data from corrupting or entering inconsistent states	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?	End user traffic (i.e. your customers submitting data via First AML's Electronic ID Verification form) is encrypted using TLS1.2.	Noted
6.13	Is data on your servers encrypted at rest?	Yes.	Noted
6.14	Is a test environment provided to test configuration changes? If so, is there an additional charge for this?	First AML's Engineering team have a test environment for testing configuration changes. This is not available to customers and based on the level of configuraiton of our system for users, is not required for this group.	Noted
Access to customer data			
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?	First AML processes Customer Data as a data processor, and holds all Customer Data as such and in accordance with the applicable legal and contractual requirements. For full details of First AML's processing activities, please see First AML's Data Processing Addendum.	Noted
6.16	Are you subject to any legal or regulatory requirements obliging you to retain a copy of customer data?	No	Noted
6.17	Who will be able to access or see customer data?	Authorised employees of First AML are able to access or see customer data where it is necessary as part of contractual necessity or legitimate interest as described in our privacy policy at firstaml.com/privacy-policy . Employee system access is reviewed quarterly and adjusted as staff leave the Company or their role changes. For your own internal users, authorised members of your team will have permission in our software to add or revoke your internal users.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
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.	<p>First AML grants user access on a least privilege basis, with defined system access permissions for each role type and access being issued by authorised employees. This ensures staff only have the level of access necessary to perform their role. Employee system access is revoked/adjusted when they leave the company or change role.</p> <p>First AML utilises MFA and other access controls where possible which reduce the chance of unauthorised access of accounts.</p>	Noted
6.19	Explain the release management procedures in place and the associated segregation of duties ?	Any changes for the platform require a number of review and approval steps to take place. The engineer submitting changes will request a code review from 1-2 additional engineers in addition to an automated test suite running against the changes. Both an approved code review, and a successful run of the automated testing is required in order for the code to be deployed. On successful code review and passing tests, the code is deployed to a staging environment for validation and additional testing. The deployment process then requires additional validation and approval to unblock the changes to production / live systems. There are three distinct roles in place with this process that can be fulfilled by subsets of engineering: change requestor, change approvers, and deployment approver.	Noted
6.20	Is there sufficient segregation of duties preventing system developers from accessing and changing live applications and data files?	Yes - only our on-call and site reliability engineering teams have production environment access.	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?	First AML utilise a co-piloting system for all emergency changes that need to be completed to live applications and data. These operations require a minimum of 2 of our senior on-call engineers. One person documents the change about to be applied and performs dry run operations to observe the expected output. The other on-call engineers review the proposed operations, and provide feedback and guidance on the change to be applied. In addition to this, we utilise code reviews for any code changes being deployed to live production systems which require a minimum of 2 engineers to approve. All requests to change live application data are captured in our messaging platform for visibility to all on-call engineers and stakeholders.	Noted
6.22	Is an audit trail always maintained of these emergency changes?	All events related to an emergency change to live production data are logged and stored in a secure logging partition with only senior on-call engineer access. This includes the engineer who executed the commands and the commands they ran. Live production application changes are always reviewed via the code review process, and approvals and comments are stored in github to assist with audit requirements	Noted
6.23	What procedures are in place when members of staff leave to ensure that their system access is stopped?	First AML has an employee off-boarding process which includes returning of all equipment, and revocation of system access which consists of cloud-based SaaS logins which are disabled.	Noted
Platform and service levels			
6.24	Which databases can be used (Hosted) or are used (SaaS)?	We utilise two main storage components in our solution for data - Amazon S3 (document storage), and Amazon RDS Postgres (a database server).	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.25	What forms of user authentication are supported e.g. user names, passwords certificates, tokens etc.?	Username and password based authentication is available to all users with some password length and complexity requirements enforced. On our Enterprise product tier, we offer SAML2.0 support through Auth0 so Companies can connect their single sign on tool such as Okta to harden and self-manage their authentication requirements.	Noted
6.26	What is the proposed product/service availability percentage?	The proposed availability percentage is 99.9% over any given monthly billing period	Noted
6.27	What percentage availability has been achieved over the past 12 months?	99.99%	Noted
6.28	Is a service level agreement ("SLA") offered regarding: - Service availability? - Data recovery?	Service Availability uptime SLA is 99.9% during any monthly billing cycle. There is no SLA offered for Data Recovery	Noted
6.29	Is the service available 24x7 or are there downtime periods for maintenance?	The service is available 24x7 with no defined downtime periods for maintenance.	Noted
6.30	Is the customer made aware of maintenance periods in advance?	If there was a maintenance event that required the platform to be offline outside of normal operating hours in New Zealand, Australia and the EU then notification would be sent to our customers in advance	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?	Our Software works entirely within the internet browser software on the user's computer.	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?	N/a - cloud based software.	-
Platform security			
6.33	What security steps are taken to prevent and detect intrusion attempts?	A variety of observability and monitoring software is involved in detecting and alerting for intrusion attempts: AWS GuardDuty,, Sumologic and Lacework. Anomaly detection via our observability looking for unusual patterns in activity (such as S3 logs) will trigger alerts notifying our on-call and security team, who then undertake further investigation.	Noted
6.34	Is firewall hardware and software used to protect the live systems from unauthorised access?	Yes	Noted
6.35	Which monitoring software is used to create alerts when intrusion attempts are suspected?	The following software is involved in monitoring and alerting for intrusion attempts: AWS GuardDuty (via SNS alerts), Sumologic (SIEM) and Lacework	Noted
6.36	Are designated staff responsible for receiving and urgently responding to these alerts?	Yes	Noted
6.37	Have clear procedures been established for identifying and responding to security incidents?	Yes	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.	Yes - we have a formalised vulnerability management program for our Software Platform where vulnerabilities have a defined time to remediate (TTR) SLA based on severity and whether or not they exist in production environments.	Noted
6.39	List the procedures and software tools in place to prevent or detect and eliminate interference from malicious code, such as viruses?	- web based application accessed via TLS1.2+ - WAF - malware scanning of file uploads - quarterly application penetration testing	Noted
6.40	Is a system log maintained by the service provider that details - User access? - User activity? - Error messages? - Security violations?	Yes	Noted
6.41	Is this log available to the customer?	This data is not readily available to Clients however we can respond to low volume ad hoc requests to supply such information e.g. to assist a customer with a forensic investigation.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
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
6.43	Is penetration testing regularly carried out by (please indicate frequency of tests): - Staff specialising in this field? - External specialists?	Our application undergoes penetration testing on a quarterly basis. This is undertaken by an independent specialist firm called Phew .	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.	Yes - all Security controls are reviewed internally at least annually with some more frequently depending on associated risk levels, changes to risks or newly identified risks, and nature of the procedure where some require more frequent review or verification.	Noted
6.46	What security reporting is provided demonstrating compliance against certification(s) and policy(ies)?	First AML is ISO27001:2013 certified and is audited annually by the British Standards Institute as part of upholding this certification. We also undertake annual internal audits which we currently outsource to an independent specialist Firm.	Noted
6.47	Are any security breaches communicated to customers?	Any breaches impacting Customers of First AML would be communicated to the relevant data controller(s) being our customer(s).	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?	- We utilise 2 main storage components in our solution for data - Amazon S3 (document storage), and Amazon RDS Postgres (a database server). Amazon S3: - Amazon s3 creates backups of any uploaded document in near-realtime in another geographic region. - All updates to documents stored in s3 is versioned. - As such we have the ability to recover to any point in time for documents, even if we experience the lost of an entire AWS region (which is a collection of 3 or more separate data centres in a single geographic location). Amazon RDS Postgres (our database server): - We have continuous backups enabled for a 35 day period, allowing point-in-time recovery (meaning we recover to any point in time within the last 35 days). - We also perform hourly snapshot backups, which are retained for at least 366 days, allowing recovery beyond a 35 day period to a granularity of the nearest hour. - Backups are replicated to a second geographic region as well, allowing recovery in case of loss of the nearest region	Noted
6.49	How frequently is a test-restore of backups undertaken?	At least once per year, last undertaken October 2022.	Noted
6.50	Can the provider restore from a backups that it has taken at a customer request?	Yes	Noted, for the platform as a whole not an individual user.
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?	N/a	-
Platform recovery			

Ref	Requirement	Vendor Response	Reviewer Comments
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?	Customer information is stored on AWS Infrastructure with a primary and disaster recovery region.	Noted
6.54	How often are these plans tested?	In relation to database recovery - at least annually. We have other plans which are tested throughout the year e.g. loss of physical office however as our Customer data is hosted on AWS Infrastructure (not our own servers), this is not applicable to this question.	Noted
6.55	How often are these plans reviewed and updated?	At least annually, and ad hoc as changes arise.	Noted
6.56	What are your: - Recovery Point Object (RPO) standards? - Recovery Time Objective (RTO) minimum standards?	Our current RPO is 1 hour, and our RTO is 16 hours.	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 times are captured in UTC and may include an optional timezone offset if relevant.	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?	Customers may request export of their Customer Data at any time during the term of the Agreement. First AML adheres to robust processes for ensuring financial and technical resilience.	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?	Yes - if customers cease to use our service, we offer a reasonable period of time for you to conduct data exportation and can also offer long term data storage at a low cost if required.	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)?	Our product is a cloud based application where production-level changes would apply to all customers. We conduct adequate testing and peer reviews prior to enacting any changes in our production environment. In the case of major changes which may impact Clients, we consult Clients prior to implementation.	Noted
6.62	Are users able to test the application before new versions go into live use?	No - First AML conducts in-house testing undertaken by our Software Engineering team. Changes to our application are influenced by Customer requirements and we undertake adequate research including engaging with some Customers prior to making material changes.	Noted. Customers provide feedback but not assistance with testing.
6.63	Are users given notice before application changes are applied to the live system?	No, First AML undertakes continuous development of its SaaS Platform releasing product improvements regularly.	Noted
6.64	Are changes delivered into the live environment "switched off" to enable users to test them before enabling them for their environment?	No however we conduct user research before implementing product changes including seeking some customer feedback and undertaking staged rollouts which may include releasing a feature to a subset of customers prior to a release to all customers.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.65	Describe what testing and QA processes are undertaken before upgrades and other changes are made live/available to customers?	We practice continuous delivery, regular integrating changes into our live platform multiple times per day. We utilise a range of automated tests (unit, integration, end-to-end and visual differencing tests) to ensure each change is tested prior to release. We also require all code changes to undergo peer-review prior to being merged, and utilise a set of non-production environments that each release is tested against prior to being promoted to production environments. Feature flags are utilised to develop new features behind, allowing progressive roll-out of completed features, utilising beta and GA groups.	Noted
6.66	If a hosted system, explain the release management procedures in place and the associated segregation of duties?	Any changes for the platform require a number of review and approval steps to take place. The engineer submitting changes will request a code review from 1-2 additional engineers in addition to an automated test suite running against the changes. Both an approved code review, and a successful run of the automated testing is required in order for the code to be deployed. On successful code review and passing tests, the code is deployed to a staging environment for validation and additional testing. The deployment process then requires additional validation and approval to unblock the changes to production / live systems. There are three distinct roles in place with this process that can be fulfilled by subsets of engineering: change requestor, change approvers, and deployment approver.	Noted
6.67	Are users informed when they next login of the application changes that have gone into live use?	First AML makes use of an in-app messaging system called Appcues to inform Customers of changes and additions to Platform functionality.	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 - customers are not generally required to take any action when software releases are made.	Noted
Subscription options			
6.69	What is the minimum level of commitment must the customer sign up to, e.g. 36 months?	We generally operate on 12 month contractual terms.	Noted
6.70	Where online payment is used, what type of security is used to protect sensitive information?	First AML takes payment via bank transfer i.e. does not process card payments.	Noted
6.71	Where online subscription / payment is used, is an invoice provided to the customer and, if so, in what format?	For customers on variable pricing, First AML invoices on a monthly basis, which includes a monthly Platform fee and usage-based charges relating to verifications undertaken. For customers on fixed pricing, they are charged an amount as per the agreed contractual terms which often involves monthly invoicing of a specific amount.	Noted
6.72	When subscriptions need to be renewed, what advance notice is provided and what is the time limit for renewal?	First AML's Customer Success team generally get in touch around 90 days prior to contract renewal.	Noted
6.73	Is there a procedure for late renewal and is there a time limit after which subscriptions cannot be renewed?	There is no time limit within which to renew a subscription for use of the Services. Customers may procure the Services at any time.	Noted
6.74	How soon after creating or renewing a subscription (if applicable) can the system / service be used?	Upon commencing use of our service, we take new Clients through an on-boarding process which our Sales team can confirm a timeframe for as this can vary. Renewals generally don't disrupt service usage i.e. you'd expect to continue having access to our service if renewing the contract within the expected timeframe.	Noted
6.75	What notifications / confirmations are provided to the customer regarding subscriptions and payments?	First AML invoices customers on a recurring basis by email.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
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?	Customers are able to access their Customer Data at any time during the term of the agreement. Agreements do not immediately terminate upon payment failure. Customers may export their Customer Data prior to termination.	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?	If customers cease to use our service, we offer a reasonable period of time for you to conduct data exportation and can also offer long term data storage at a low cost if required.	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?	Customer data can be permanently deleted upon request, with our Engineering team actioning such requests in a permanent and GDPR compliant fashion. We can provide written confirmation of permanent data deletion once undertaken.	Noted
6.79	What is your processes regarding disposal of end-of-life and failed hardware devices that were used to operate your service?	We do not utilise any hardware devices to run our service. All components are virtual running in Amazon Web Services	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 accessible from within our cloud based software. We utilise a sub-processor Sisense to provide some of our reporting functionality.	Noted
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	Noted
6.82	What browser versions are support: - On desktop/laptop (PC, Mac, Linux)? - On Tablets? - On mobiles?	Web-based solution, supported browser versions are: - Edge - version 79+ - Chrome - version 79+ - Safari - version 13.1+ - Firefox - version 72 + Internet explorer is not supported.	Noted
6.83	Is access to the reporting facilities and data controlled by the same procedures as access to the main application?	Yes - once users are logged in to our Software Platform, they can access the reporting function if they have been allocated a suitable user role (with reporting privileges).	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?	Reports are displayed within our cloud based software and downloadable as CSV files. Verification reports can be exported as PDF.	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?	Reports are dynamically generated on demand, and can be downloaded as CSV to a user's 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?	No	Noted
6.88	Are communications between the browser and the server encrypted for any report related communications?	Yes	Noted
6.89	If reports are produced dynamically each time the user views them can historical reports be reproduced at any time?	No	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.90	Can reports viewable in a browser be navigated dynamically by users? For example: <ul style="list-style-type: none"> - Enabling drill down to more detailed information? - Altering which columns and rows of data are displayed. - Choosing time periods? - Specifying selection criteria? 	Yes	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?	No - but a CSV can be downloaded then data could be pasted from there if required.	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?	An error message would be displayed if the reporting tool was not able to retrieve information.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.	ANTI MONEY LAUNDERING		
Global setup			
7.01	Does the system make use of global lists, e.g.: - Postcodes? - Client [business/firm] types? - [Accountancy] firm service lines and sub-services? - Other, please specify?	For individuals (clients) completing AML checks, we use a global address lookup for auto-complete, plus we use a library for phone numbers, storing them in E.164 format. We do not make use of any other lists, such as firm types or accountancy services.	Noted, as selected by FirstAML
7.02	Does the system have an audit trail that includes details of: - Changes to standing data (global lists)? - All manual entries/changes to inputs made by a user? - All items deleted from e.g. a Risk Assessment? - Information that has been uploaded? - Information provided by third-party suppliers? - All authorisations/approvals?	Our platform maintains an audit trail of all data updates, whether these are automated or manually made by our users. All information uploaded or obtained by third-party providers is uploaded and securely stored in our ecosystem.	Confirmed
7.03	Can the system operate in multiple currencies? If so: - Please state which are supported. - Confirm whether any additional (third party) services can be purchased in other currencies.	We do not offer transaction-based services in our product	N/A
7.04	Does the system support multiple languages?	No - We don't provide our platform in any language, other than English, at present	Noted
7.05	Does the system provide inbuilt workflow functionality?	We automatically send reminders to individuals we have requested to electronically verify and to end-users who have been requested to provide us with documents for the purpose of verification. These trigger after a period of inactivity. Notifications are sent to the Reporting Entity (our customer) when a case is ready for them to review.	Confirmed
7.06	Does the system allow a user to use multiple devices to support mobile working, e.g. a workstation, phone and/or a tablet?	Yes. Our system is a web-based product which supports multiple browsers and devices including workstation, phone and tablet.	Confirmed
7.07	Does the system provide a facility for auto-saving changes 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?	Information we require our customers to input into our platform is minimal, and is usually contained to a single editable field or modal which mostly negates the need for auto-saving functionality. History / states are not currently able to be rolled back.	Confirmed
7.08	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?	Our web-based product does not support an offline mode. We do offer an API which would enable firms to implement a solution which included supported offline activity.	Noted
7.09	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, etc): - Banks and other financial institutions? - HMRC? - Accounting software (e.g. Sage, QB, Xero)? - Tax software? - Pension software? - Credit check agencies? - Providers of DBS checks? - Others, please specify?	For our UK customers, our software directly integrates with the following services via their APIs for identity verification and screening. - FrankieOne - Onfido - ComplyAdvantage - GDC (available soon) We also have a direct integration with a BI reporting provider, Sisense. We have a series of reporting dashboards that are fully-embedded into our platform via an SDK	Noted. The four stated are the main data source providers currently used.
7.10	Does the system provide a portal to enable the exchange of information between the Accountant and their Client(s)? Notes that the phrase: "Accountant" will be used for the firm of Accountants having individual users of the software, and "Client" will be used for the customer of the accounting firm on whom the AML compliance checks are being run.	Yes, our portal allows the Accountant to collect Client information directly in person. Most commonly, our portal enables the Accountant to provide their Clients contact information to our AML Specialists, who then use our system to facilitate the exchange of information between the Client and Accountant.	Noted. There is a video that shows how a QR code is used to do this.

Ref	Requirement	Vendor Response	Reviewer Comments
7.11	<p>If yes, please clarify the level of security in relation to:</p> <ul style="list-style-type: none"> - How authentication is managed? - Whether Multi Factor Authentication (MFA) is supported? - Is a secure [https:] connection provided? - Are login / inactivity timeouts enforced? - Are complex passwords required as well as the need for regular password changes? 	<ul style="list-style-type: none"> - Authentication is managed via username and password with complex password requirements, including use of an industry-leading IDaaS product to implementate Authentication (Auth0) which includes additional mechanisms to identify compromised passwords, brute force protection etc. - Other factors (such as change of a devices location/country/IP address) will also cause a user to need to reauthenticate as a security precaution. - Product can be integrated into a customers existing user directory (SSO) which allows them to employ MFA or other controls as supported by their user directory. - For Customers without their own internal SSO service, additional MFA options and Social login support (google,apple,microsoft) login options are being released in next 2 quarters. - Yes, https connection is provided. - Users are automatically logged off after a pre-set idle time. Currently the time period is not customer configurable. 	Noted
7.12	<p>What end-user computing platforms are supported for access, e.g. Windows, Mac, iOS, Android? And what Internet Browsers are supported?</p>	<p>Our web portal supports the following web browsers across all common computing platforms:</p> <p>Desktop:</p> <ul style="list-style-type: none"> - Edge starting from their migration to Chromium - 79+ - Chrome 79+ - Safari 13.1+ - Firefox 72+ <p>Mobile/Tablet:</p> <ul style="list-style-type: none"> - Chrome 79+ - Safari 13.1+ - Firefox 72+ - Samsung Internet (latest version) 	Noted
7.13	<p>What Accessibility standards have been adhered to in the design of the portal?</p>	All our designs follow the Web Content Accessibility Guidelines (WCAG) 2.1 standards	Noted
Firm setup and registration			
7.14	<p>On first use, do the details entered as part of the on-line registration process, automatically pre-populate the Accountancy Firm's "Firm" details within the system?</p>	Firms are setup in our system by our implementation specialists during onboarding.	Noted. This is done by the FirstAML onboarding team.
7.15	<p>If so, is there the option to subsequently amend the Firm details?</p>	N/A	-
7.16	<p>Can the services undertaken by the Accountancy Firm be selected from a master-list so as to define the areas of operation (and thus operational risk) of the firm?</p>	<p>Standard Operating Procedures are established and agreed during implementation and outline how we collect and process information on your behalf, and our methodology for conducting CDD/AML.</p> <p>Depending on AML legislation, some features are configurable according to the our customers' own compliance program. For example, Adverse Media & Continuous Monitoring can be enabled or disabled in certain product tiers according to customer preference.</p>	Noted. The SOP is available under "Legal" on FirstAML's website. This sets out the workflow that will be followed by FirstAML and the Accountancy firm.

Ref	Requirement	Vendor Response	Reviewer Comments
7.17	Can the selected services be amended if the Firm changes what it offers to its clients? If so, is a dated history maintained of the services selected?	Deviations from the SOP are possible, depending on the nature of the customer's requirements. Platform feature configuration can be amended as required according to the customer's eligibility for those features. Dated history of configured services is not presented within the platform but is maintained in our audit logs and our billing platform if billing is impacted.	Noted. Sometimes FirstAML needs to try and align the SOP with a firm's own AML policies.
7.18	Does the system provide an introductory workflow to ensure that the key firm compliance and user security procedures are in place before the system is used to manage clients and undertake client risk assessments? If so, please explain what is provided?	Our AML Specialists and Customer Success team can provide comprehensive assistance to help ensure key compliance procedures are in place, and that customers are kept across legislation changes.	Noted. The FirstAML onboarding team will outline the workflow.
7.19	On first use does the system come pre-populated with a global (administrator) account, with the ability to setup and manage an Money Laundering Reporting Officer ("MRLO") account?	Yes, user accounts are setup by our implementation specialists during onboarding. Many user roles are available including admin and MLRO / Compliance Officer roles.	Confirmed; these are roles that can be set against users.
7.20	Must the MRLO [user] be created before firm and client risk assessments can be undertaken?	N/A - our platform does not currently support risk assessments	Noted. The FirstAML focus is "AML Onboarding" / KYC / CDD rather than AML-related risk assessments.
7.21	Must a firm risk assessment be undertaken before client risk assessments can be undertaken?	N/A - our platform does not currently support risk assessments	Noted
7.22	Does the system have the ability to provide third-party verification services from within the platform?	Yes	Noted
7.23	If so, can the results be recorded against the clients on whom verification has been requested?	Yes, verification and screening results are recorded against the client.	Confirmed
7.24	What third-party services are integrated: - Client [contact] verification? - Client [company] verification? - Digital biometric verification? - Company House firm-details? - Other, please specify?	For our UK customers, we are directly integrated with the following services: - Client [contact] verification - Digital biometric verification - ID verification (including document anti-tampering checks) - Client screening checks (PEP, Sanctions, Adverse Media) Our AML Specialists also conduct Client [company] verification & Company House firm-details	Noted; see 7.09 above.
User management			
7.25	Does the system provide for the setup and maintenance of the details of the users (the individuals in the Accounting firm) using the software?	Yes, we offer a "Platform Admin" role which provides the ability to invite firm users and manage their permissions and status.	Confirmed
7.26	If yes, does the system enable the user to change their own details and change their password?	We allow users to change their password, but not update their name or email address	Noted
7.27	Does the system provide a permissions matrix so that rights can be set at user and role/group level? If so, does this provide at least the following levels of security: - An administration/global user who can setup the MLRO? - The MRLO, who administers other users and authorises any AML documentation sent for approval. - A normal user, who undertakes the AML checking process for clients. - Other levels, please specify?	Yes, we offer different roles within our platform that include platform administrators, MLRO (compliance officer) and other various roles to support creating, viewing, approving and auditing activities across multiple offices/teams. See here for more information: https://firstamlsupport.freshdesk.com/support/solutions/articles/69000305862	Confirmed
7.28	Can multi-level authorisations be set? E.g. A user and their manager must both approve an action; or perhaps the user and the MLRO?	Multi-level authorisations aren't currently supported.	Noted
7.29	Does the software allow a user to assign a "delegate", who has access to view/amend a sub-set of the full information entered into a risk assessment? If yes then please explain the levels of access provided.	We offer specific roles that support the ability to view/submit information as part of a risk assessment (excluding access to other teams/offices, or approval capabilities), but we currently do not support the ability to delegate or assign activities to other firm users.	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.30	Can a separate user account be created specifically for a "regulatory body" which provides read-only access to the data for audit purposes? If so, please explain what is provided.	Yes - we provide an "auditor" role. This is a read-only role that has access to all case data relating to a reporting entity. This role can be revoked once the regulatory body has completed their assessments.	Confirmed
7.31	Can users be "archived" if they are no longer active within the Accountancy 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? - Must a subscription still be paid for an archived user?	Yes, users can be de-activated within the platform by the "Platform Admin" role. - This history is not currently maintained / visible in the platform. - Yes, deactivated users can be reactivated - No, users are not tied to platform pricing	Confirmed; there is a flag against the user to set active on/off.
7.32	Are there restrictions on more than one user at the Accountant working on the same client risk assessment at the same time?	N/A - our platform does not currently support comprehensive client risk assessments at this time. Each "case" in our platform contains an input field where the risk assessment result can be stored. This field contains the following values: High, Medium, Low	Noted
7.33	Are there restrictions on one user at the Accountant working on multiple risk assessments (for different clients) at the same time?	N/A - our platform does not currently support comprehensive client risk assessments at this time. Each "case" in our platform contains an input field where the risk assessment result can be stored. This field contains the following values: High, Medium, Low	Noted
7.34	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?	Users can see their profile visible in the portal, which includes their name and email address. Users are able to log out of their session and log back in using different username and password, if they have been provided with multiple user roles with differing permissions.	Confirmed
Internal AML training			
7.35	Does the system have an in-built training module that logs whether staff have undergone firm-mandated AML training and read [and agreed] to the firm's latest AML policy?	No our platform does not currently offer this.	Noted; CPD is not provided but a comprehensive set of videos are available.
7.36	If yes: - Is full history of training modules undertaken kept with each employee? - Are there associated tests with the training modules?	N/A	-
7.37	Is the need to undertake this training forcibly refreshed periodically or as the system or regulations are updated?	N/A	-
7.38	Are users blocked from undertaking client risk assessments if they have not passed mandatory tests?	N/A	-
7.39	As training modules are updated are users prompted to update their learning?	N/A	-
7.40	Does the system have a library of AML-related training and help accessible to users of the system? If yes, are these kept up to date by the service provider to ensure that they meet the latest legislation?	We have a comprehensive Help Center and ticketing system available to users of the platform, which is kept up to date as we release and enhance platform features.	Confirmed
The Firm's AML policy			
7.41	Does the system provide a AML Policy template that the Firm can tailor and save as the Firm's "Standard"?	No	Noted
7.42	Can updated versions of the default template be uploaded when provided by the vendor; with changes easily identified to make for simple updating of the Firm's Standard?	N/A	-
7.43	Can individual sections of the Policy be amended separately, rather than the whole document needing to be changed in one go?	N/A	-
7.44	Is a history of changes retained in the system?	N/A	-
7.45	If the Firm's AML Policy is updated, are users required to read and acknowledge this the next time that they use the system?	N/A	-
7.46	If so: - is this logged in their training record? - Is it possible to see easily which users have yet to acknowledge the new version?	N/A	-
The Firm's AML risk assessment			

Ref	Requirement	Vendor Response	Reviewer Comments
7.47	Does the system provide an inbuilt Risk Assessment for the Firm itself, based on the areas of work defined in section 7.15 above	No - our platform does not currently support comprehensive risk assessments at this time. Each "case" in our platform contains an input field where the risk assessment result can be stored. This field contains the following values: High, Medium, Low	Noted
7.48	Are the Firm Risk Assessment questions for the various different services provided by Accountancy firms included as part of the platform? If so, list the main areas included.	N/A	-
7.49	Are some questions in the Risk Assessment mandatory and others optional depending on the services selected by the firm?	N/A	-
7.50	Does the system show progress through the Risk Assessment: which sections have been started and which completed?	N/A	-
7.51	Does the system allow subsequent amendment of individual entries, without the need to walkthrough complete sections of questions again?	N/A	-
7.52	Does each question have its own 'high' or 'low' risk outcome depending on the answer, and provide notes of the steps that could be taken to address each of the high risk outcomes?	N/A	-
7.53	Do all the questions have additional guidance and useful links should further clarification be required by the user?	N/A	-
7.54	Is a comments box available under each question, to provide the facility to capture additional information relevant to the Firm Risk Assessment?	N/A	-
7.55	Are suggested risk mitigation steps included against each question?	N/A	-
7.56	Are high risk areas clearly highlighted?	N/A	-
7.57	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?	N/A	-
7.58	Does the system log the completion of the various sections of the input forms once all questions in a section have been completed?	N/A	-
7.59	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?	N/A	-
7.60	Can a completed section be manually marked as not completed?	N/A	-
7.61	Does the system have search functionality to enable the user to jump to a specific question?	N/A	-
7.62	If a question is answered as a 'no', does the system allow the entry of a suggested mitigation by the user?	N/A	-
7.63	If so, is the MRLO alerted to this and do they have the option to accept/reject the suggested mitigation action?	N/A	-
7.64	If all high risk answers for the Assessment been accepted as 'mitigated' then will the Firm move from the high risk category, to the risk mitigated category?	N/A	-
7.65	Does the system provide: - A viewable answer history? - An audit trail of answers and changes to answers? - A PDF report of the risk assessment? - Other reports, please specify?	N/A	-
Client setup			
7.66	Does the system provide for the setup and maintenance of the general details of the Client? If so, does this include: - Company name and company number - Address - Contact information - A flag denoting whether the Company is active or not? - Beneficiary details - Contact details	Our portal allows the basic details of clients and entities requiring verification to be provided when creating a Case. Profiles for individuals and entities are not currently supported but is likely in the near future.	Confirmed
7.67	Can client/company information be imported using a standard spreadsheet template? If so, how is this validated?	No	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
7.68	Can document files be uploaded against a client [to support the Risk Assessment]? - If yes, what format of files is supported, e.g. PDF?	Yes, we allow documents to be uploaded for individuals and other entities via the case. - A wide range of documents are supported including PDF.	Confirmed
7.69	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 downloaded individually or all at once for an individual or case. - Marking as reviewed/approved not currently supported	Noted
7.70	Can a client be flagged as archived, so that new risk assessments cannot be undertaken? If so, can an archived client be unarchived by a user with sufficient security privileges?	Not currently, but likely when profiles are supported for individuals and entities	Noted
Client risk assessments			
7.71	Does the system contain a series of client risk assessment templates that cover different client types, e.g. Limited, Company, Charity, Partnership, Trust, etc	N/A - our platform does not currently support comprehensive client risk assessments at this time. Each "case" in our platform contains an input field where the risk assessment result can be stored. This field contains the following values: High, Medium, Low	Noted
7.72	Can a client Risk Assessment type be selected based on the type of company that the client is identified as during its setup? If so, is the type of the associated Risk Assessment selected automatically by the system based on the details entered previously?	N/A	-
7.73	Do the client Risk Assessments provided cover all the areas of work selectable during the Firm setup process, see section 7.15 above	N/A	-
7.74	Are some questions in the Risk Assessment mandatory and others optional depending on the services selected by the firm?	N/A	-
7.75	Does the system show progress through the Risk Assessment: which sections have been started and which completed?	N/A	-
7.76	Does the system allow subsequent amendment of individual entries, without the need to walkthrough complete sections of questions again?	N/A	-
7.77	Does each question have its own 'high' or 'low' risk outcome depending on the answer, and provide notes of the steps that could be taken to address each of the high risk outcomes?	N/A	-
7.78	Do all the questions have additional guidance and useful links should further clarification be required by the user?	N/A	-
7.79	Is a comments box available under each question, to provide the facility to capture additional information relevant to the Firm Risk Assessment?	N/A	-
7.80	Are suggested risk mitigation steps included against each question?	N/A	-
7.81	Are high risk areas clearly highlighted?	N/A	-
7.82	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?	N/A	-
7.83	Does the system log the completion of the various sections of the input forms once all questions in a section have been completed?	N/A	-
7.84	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?	N/A	-
7.85	Can a completed section be manually marked as not completed?	N/A	-
7.86	Does the system have search functionality to enable the user to jump to a specific question in the information collection process?	N/A	-
7.87	If a question is answered as a 'no', does the system allow the entry of a suggested mitigation by the user?	N/A	-
7.88	If so, is the MRLO alerted to this and do they have the option to accept/reject the suggested action?	N/A	-

Ref	Requirement	Vendor Response	Reviewer Comments
7.89	Do the answers made to the questions in an Assessment indicate whether simplified, standard, or enhanced due diligence is required (i.e. is the criteria built into the questions in the Assessment), and adjust the questions sets [and number of questions] accordingly. See also " Checking Clients " below.	N/A	-
7.90	If all high risk answers for the Assessment been accepted as 'mitigated' then will the Firm move from the high risk category, to the risk mitigated category?	N/A	-
7.91	If the answers made to questions indicate that the client is classified as "high risk" [*] does the system require additional Enhanced Due Diligence ("EDD") questions to be answered? [*] - In a high risk ovation/jurisdiction - Identified as a Politically Exposed Person (PEP) - Where there is a high risk of ML or terrorist activity.	N/A	-
7.92	Does the system provide: - A viewable answer history? - An audit trail of answers and changes to answers? - A simple summary of the answers falling into high/low risk and mitigated/non-mitigated categories?	N/A	-
Editable and re-usable client risk assessment profiles			
7.93	Does the system allow the Firm to create their own Client Risk Assessment profiles?	No - our platform does not currently support comprehensive client risk assessments at this time. Currently, for a given case (which contains Clients), our system allows capture of an AML profile including: Captured activity; Purpose; Nature; Risk Assessment (Low, Medium, High); CDD Level (Simplified, Standard, Enhanced); Transaction value	Noted
7.94	If so: - Does the system include a rules engine to help create appropriate questions and resulting risk ratings? - Can the rules link to the results of client identify checks (see below) - Does the engine allow the generation of risk scores, which can then trigger additional questions (EDD)?	N/A	-
7.95	Does the system provide the option for an authorised user in the Firm to manually amend a Client Risk Assessment template?	N/A	-
7.96	If so, can the amended template be saved as: - The new default for that client type? - A selectable template for that specific client? - A selectable template for a number of clients? - A default template for one or a number of clients? - Other, please specify?	N/A	-
7.97	Does the system provide the option for an authorised user in the Firm to manually prefill answers to the questions in a Client Risk Assessment template, and then save this template for [re-]use on similar clients, e.g. those in a similar industry? If so, is there an additional cost for this feature?	N/A	-
7.98	If so, can the amended template be saved as: - The new default for that client type? - A selectable template for that specific client? - A selectable template for a number of clients? - A default template for one or a number of clients? - Other, please specify?	N/A	-
Client identity checking			

Ref	Requirement	Vendor Response	Reviewer Comments
7.99	Is the client checking process undertaken: - By the Accountancy Firm's own users? - By the supplier once the client's details have been entered? - By the Accountancy Firm but with the option of assistance from the supplier if required (at an additional cost)? - Other, please provide details?	By the supplier once the client's details have been entered	Confirmed
7.100	Does the system provide integrated identity checking functionality?	Yes	Confirmed
7.101	If so: - What third-party providers are used? - Is a separate/additional subscription required?	For our UK customers, FrankieOne is used for client identity verification. GDC will also be used for this purpose in future A separate subscription is not required.	Noted
7.102	Can the results of a check be saved against the client record together with the data of the check and originating user ID?	Yes, results of a check are saved against the client record along with any relevant data and the date of the check.	Confirmed
7.103	Does the system provide integrated biometric ID verification functionality?	Yes	Confirmed
7.104	If so: - What third-party ID providers are used? - Is a separate/additional subscription required?	Onfido is used for ID and biometric verification. A separate subscription is not required.	Noted
7.105	Can the results of a check be saved against the client record together with the data of the check and originating user ID?	Yes, results of a check are saved against the client record along with any relevant data and the date of the check.	Confirmed
7.106	Is there a time-window within which these checks must be undertaken once the process has been started?	Generally, no. However, once First AML receives a case from the Firm, if there is no activity on the case from the Firm or Client for 30 consecutive days, the case will become dormant.	Noted. This is part of the SOP.
7.107	Does the system provide functionality to check the identity of a client where that client/customer is not a private individual, but rather an organisation? If so, does this allow for the identification of the organisation's ownership and who has control.	Yes, our solution is able to verify organisations, and will identify the individuals in that organisation with a controlling stake.	Confirmed
7.108	Does the system provide an integrated link to Companies House in order to verify company details?	An integrated link is not available, although any relevant information is made available for customers in our platform by our AML Specialists.	Noted
7.109	If so: - Is the link direct to Companies House or via a third-party provider? - Is a separate/additional subscription required?	N/A	-
7.110	Does the system provide any third-party links for checking overseas companies? If so, please provide details	An integrated link is not available, although any relevant information is made available for customers in our platform by our AML Specialists.	Noted
7.111	Can the results of a check be saved against the client record together with the date of the check and originating user ID?	Yes, results of a check are saved against the client record along with any relevant data and the date of the check.	Confirmed, saved as part of the case profile.
7.112	Does the system provide an integrated link to third-party companies providing credit-checking functionality?	No, credit checking is not currently supported.	Noted
7.113	If so: - Is a separate/additional subscription required? - Can the results of a check be saved against the client record together with the data of the check and originating user ID?	N/A	-
7.114	Does the system have a set of standard emails that can be used to request client identification related documents and/or provide authorisation from individuals for information searches?	We offer an Electronic Identity Verification (EIV) form that can be used to request client identification, collect documents and biometrics, along with client authorisation. We also offer a secure web form to collect other certified documents that may be required. These can be sent via email or the client can be provided with a URL.	Confirmed

Ref	Requirement	Vendor Response	Reviewer Comments
7.115	Is an audit trail retained of the requests made and emails sent? If so, does the system provide the facility for an internal approval to be undertaken and recorded against each?	Yes, all emails sent via the platform are recorded. As these are "templates" that are not currently able to be edited by the Firm, there is no facility for approval to be recorded against these.	Noted
7.116	<i>LEFT INTENTIONALLY BLANK</i>		
7.117	Does the system have the facility to produce documentation on a clients that shows: - Entity structures? - The ultimate beneficial owners?	Yes. Our system visualises the entity structure and beneficial owners.	Confirmed, the entity structure tab shows this.
7.118	If so, does this cover: - Individuals? - Companies? - Trusts? - Pension Funds? - Sole Trader? - Other entities, please specify?	Yes, our system supports the verification of over 30 entity types.	Confirmed
7.119	Does the system have a database of pre-verified entities? If so, is this updated by the supplier on a regular basis?	Our system allows entities we have already verified to be retrieved for subsequent cases, if we have recorded consent from those entities.	Noted
7.120	Is the user able to drill down/across into the entity structure and view the details at each level?	Yes	Confirmed. Easy drill through to the details is provided.
7.121	<i>LEFT INTENTIONALLY BLANK</i>		
7.122	Can a user report/refer a client to the Firm's MLRO? If so, is further user activity on that client blocked until unblocked by the MRLO?	No. We support multiple roles that provide different levels of view, read and write access, but don't yet have escalation capability within Firm roles.	Noted
Dashboard			
7.123	Does the system incorporate dashboard functionality such that the current status of client Risk Assessments can be presented to the Accountant on a single screen, showing: - Client and client type (Risk Assessment type)? - Progress of any current assessment? - Historic Risk Assessments undertaken for that client? - Whether there are outstanding reminders/actions? - Whether there are associated documents logged in the system? - Other, please detail?	Yes, we have dashboard functionality available in both the platform and our embedded reporting portal. Both allow for the viewing of cases by status, who the client is and what vertical they are a part of. Our reporting function allows for the viewing, sorting, downloading and exporting of all data held against a case, individual or entity. Against each case, the user is able to download all documents associated with that case.	Confirmed
7.124	If so, can the Accountant navigate directly from the dashboard into: - A historic or currently open risk assessment? - Any outstanding reminders/actions? - A view of the company structure and beneficial owners? - Other, please specify?	From the reporting dashboard, the user can click into a single case/individual/entity record where they are able to easily understand the progress of the case through the activity logged against that case. Against all cases that have associated entities the user will be able to view the structure of entities and related individuals.	Confirmed
7.125	Is the Accountant able to share the dashboard with the Client? If so, explain how this operates.	No, not currently	Noted
Reports			
7.126	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.	Our platform provides self-serve reports that allow firms to view, filter, sort and export to csv the data held in the platform. We currently have reports on cases, individuals (clients) and entities. Reports can be filtered by date(s) - created, completed etc, status, office location, individual screening etc	Confirmed
7.127	Does the system allow drill through from a report into the underlying Assessment section/question?	Yes	Confirmed

Ref	Requirement	Vendor Response	Reviewer Comments
7.128	Are all reports adequately titled and dated? e.g. report name, Client name, pages, numbers etc.	Yes	Confirmed
7.129	Do the reports provide totals where applicable?	No - data can be sorted, filterd and exported for more detailed analysis.	Noted
7.130	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	No, not currently	Noted
7.131	If so, does the system allow graphics and/or Participant logos to be incorporated in the page formatting?	N/A	-
7.132	Can all reports be print previewed?	No	Noted
7.133	Does the reporting functionality have the facility to scroll up and down when output to screen?	Yes	Noted
7.134	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.	Yes we allow reports to be exported to .csv	Confirmed
7.135	Explain how a report [or parts of a report] can be published/provided to the Participant.	All reports can be downloaded to csv and provided	Noted