


<b>HEADER</b>		
	ICAEW Technical Accreditation Scheme "Digital Client OnBoarding" Software Evaluation	
	<b>Verify by Tiller</b>	
		
	Date completed: 26th January 2023	
	© ICAEW. Technical Accreditation Questionnaire v Z118	
<b>CONTENTS</b>		
1	Introduction and Prologue	
2	Issues identified and evaluation conclusion	
	-- GLOBAL REQUIREMENTS:	
3	Access and Security	
4	Data processing and reporting	
5	Usability	
6	Hosted and SaaS operation (if applicable)	
	-- SPECIFIC REQUIREMENTS:	
7	Digital Client OnBoarding	

Ref		Vendor Comments	
<b>1.</b>	<b><u>INTRODUCTION AND PROLOGUE</u></b>		
<b>Introduction</b>			
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	<p>Fundamentally, good software should:</p> <ol style="list-style-type: none"> <li>1. Be capable of supporting the functions for which it was designed.</li> <li>2. Provide facilities to ensure the completeness, accuracy, confidentiality and continued integrity of these functions.</li> <li>3. Be effectively supported and maintained.</li> </ol> <p>It is also desirable that good software should:</p> <ol style="list-style-type: none"> <li>5. Be easy to learn, understand and operate.</li> <li>5. Make best practical use of available resources.</li> <li>6. Accommodate limited changes to reflect specific user requirements.</li> </ol> <p>It is essential, when software is implemented, for appropriate support and training to be available.</p>		
<b>Approach to Evaluation</b>			
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.		
<b>Prologue: Matters to consider before purchase</b>			
1.08	General Overview:	Verify by Tiller is the convenient, streamlined way to collect and verify KYC information from your customer. Designed for the rigours of regulated and supervised businesses globally, Verify makes performing KYC checks simple, secure and cost-effective.	
1.09	Supplier background:	Tiller Technologies was founded by people who have worked as regulated persons across financial industries. Our sister company was an FCA regulated company and utilised the same core technology. Tiller is a Jersey-based company, located in arguably the epicenter of international companies onboarding international customers. Our development staff are mainly based in the UK but with additional staff now based in N. Ireland and India.	

Ref		Vendor Comments	
1.10	Product background and suitability for the user:	Verify by Tiller was specifically designed to meet the needs of regulated or supervised companies in the UK or internationally, that need a high quality, dependable solution for collecting and verifying customer identity for KYC purposes. The system allows client firms to be up and running same-day, via a simple self-service signup and bypasses the need for internal IT integration or other complex setup. For accountants, the system provides your customers with an effortless way to provide proof of ID & residential address within a few minutes - thereby eliminating a frustrating and time-consuming part of the onboarding process.	
1.11	Add-on modules:	Currently the system allow a firm to collect and verify a customer's ID document (passport, ID card or driving licence) from approx 150 countries. It also provides an automated address verification process (by accessing 'regulatory-quality' online databases, e.g. utilities, credit agencies, and gov. sources). It also includes a 1-time PEP & Sanction screen. Our launch proposition defaults is that all checks are included as standard, but future rollouts will allow the client firm to select services on a modular basis. The first add-on module will be a UK bank check function, which allows the firm to check the customer's account details are valid, the account is open, and can accept/pay out monies. We will continue to add on functionality over time such as the ability to collect more information on the customer via expanded enquiry forms.	
1.12	Typical implementation [size]:	The design of the system means that it appeals to firms of all sizes. We have firms as small as 1 person, up to global institutions who are interested in working with us, such is the universal use-case. The key attractions are no up-front charges, no integration requirements, and PAYG pricing per use. On average the typical accountancy firm we are signing up is 5-20 employees.	
1.13	Vertical applications:	No vertical integrations are required as the system is designed to work without integration.	
1.14	Server platform and database:	Verify by Tiller uses Microsoft Azure public cloud services. The client firm is not required to have additional servers or databases	
1.15	Client specification required:	Verify by Tiller facilitates self-serve signup by the client firm. We require only minimal details to complete the signup - eg company name & registration number, address, website & logo. Client firms can make use of all web browsers.	
1.16	Partner network:	We are developing our partner network at present - however, given the self-service nature of the product, most client firms are happy dealing direct with us.	

Ref			
2.	<b>ISSUES AND CONCLUSION</b>		
<b>Highlighted issues</b>			
2.01	<b>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:</b>		
2.02	Findings for considerations by potential customers: (See vendor comments against the various Questions)		
	* The system does not integrate with Microsoft's Active Directory for single sign-on.		3.08
	* No multi-factor authentication, although this is on the roadmap for later in 2023.		3.09
	* Backup and recovery are functions designed for disastery recovery of the platform; not for recovery of data for individual customers.		3.28
	* Files cannot be uploaded and stored generally within the system; although specicifc documents may be uploaded if required for a verification.		4.15
	* Curently data import is not supported. However import formats are planned fror future releases.		4.17
	* There is no internal report generator. The final verification output is prduced by the system as a PDF. There is also no library of reports and users cannot create their own reports.		4.30-4.37
	* The system is currently only available in English; although it has been designed to be multi-lingual in future.		5.01
	* Only limited customisable branding is available.		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; although these are really not necessary.		5.10, 5.13
	* There is no universal seach facility; but again this is really not required.		5.15
	* The user manual/help is not editable by the end-user.		5.22
	* ESCROW is not provided. Note that this is not unusual for this sort of software [subscription] service.		5.23
	* No current links between the software and other packages inc links to spreadsheets; however this is not required.		5.41, 5.42
	* Whist a pubished SLA sets out Tiller's servoce level objectives there us no guarantee provided relating to service availability.		6.28
	* It is not possib;e for a customer to take their own backups.		6.51
	* Users are not able to test new versions before they go live. Note that this is not uncommon for SaaS platforms.		6.62
	* Reports are currently only produced in PDF format; with other formats planned for future releases.		6.85
	* The system only supporte English at present.		7.03
	* Whilst bank acocunt verification is not currently provided this is on the development roadmap for Q2 2023.		7.07 7.59-7.60
	* Single sign on is not currently supported; but also on the roadmap for 2023.		7.12
	* Authorisations, delegated access and multi-level authorisations are not supported; but are not really required.		7.16, 7.17, 7.18
	* Import of contact details via spreadsheet is not supported; but Tiller state that this may be considered for a future release.		7.23
	* Note that the system supports verification of individuals and not of companies/organisations.		7.43 to 7.46, 7.49 to 7.52
	* Verification of whether a PEP or Sanction match is a false positive must be performed outside the system.		7.54

Ref			
*	The system does not provide other checks such as credit checking or UK DBS.		7.61-7.62
*	The system does not allow for user-customisable document formatting, or preview of the document being created.		7.72
<b>Evaluation conclusion</b>			
2.03	<p>For the specific use-cases in support of accountancy firms providing digital client onboarding services to their individual clients, for which the product is designed, it is a solid and capable solution. It continues to be actively developed and enhanced.</p> <p>Members should be aware of the limitation of the solution as above, and fully understand the role that it can play in an engagement.</p> <p>* 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 *</p>		
2.03a	<p>Note that the supplier makes it clear that their platform's focus is to provide assistance with client onboarding/verification as opposed to AML-related risk assessments.</p> <p>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.</p>		
<b>Disclaimers</b>			
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
<b>3.</b>	<b><u>ACCESS AND SECURITY</u></b>		
<b>Access control</b>			
3.01	What security features are included to control access to the application?	Application sign-on is via Django authentication system framework. All point-to-point communications is encrypted using HTTPS TLS encryption, and passwords one-way encrypted using PBKDF2 SHA256 algorithm. Access control is role based on the user's session privileges	Noted
3.02	Can access to functions be managed via a permissions matrix so users can only see (in menus and other links) and access those areas they are authorised to access?	Yes, Role-based permissions, based on the role access privileges, determine the functions and data which can be accessed	Confirmed
3.03	Is this access to the application managed by:- - Individual user profiles? - User groups or job roles?	Access is determined by the Role (user group) that the user profile is configured for	Confirmed. Users are either "Admin" or "Staff" users.
3.04	Can a report be produced detailing all current users, their user groups if relevant, and their authority levels and/or access rights?	An extract of users and their roles can be requested from the support team	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?	Yes, only functions for which the user has permissions for are accessible	Confirmed
3.06	Does security allow for access to be limited to: - Read only? - Read/write? - Read/amend/delete?	Depending on the function in question, yes	Confirmed
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?	Access is not permitted by any separate service or reporting tool.	Noted
3.08	Does the system security integrate with Microsoft's Active Directory or other tools that provide a single sign-on?	No	Noted
3.09	Does the system provide multi-factor authentication (MFA)?	Not at present, however this feature has been prioritised for release in Q1 2023	Noted
<b>Passwords and access logs</b>			
3.10	Is access to the software controlled by password?	Yes	Confirmed
3.11	Does each user have a separate log on (user id)?	Yes	Confirmed
3.12	If there is no password facility please state how confidentiality and accessibility control is maintained within the software?	n/a	-
3.13	Are passwords masked for any user logging in?	Yes	Confirmed
3.14	Is password complexity available and enforced?	Password complexity is enforced as follows: at least 12 characters at least 1 uppercase character (A-Z) at least 1 lowercase character (a-z) at least 1 digit (0-9) at least 1 special character not more than 2 identical characters in a row (e.g., 111 not allowed)	Noted
3.15	Are passwords encrypted?	Yes with PBKDF2 (Password-Based Key Derivation Function v2) cryptographic algorithm	Noted
3.16	Are users automatically logged off after a pre-set idle time? <del>not using the system?</del> - Can the time period be changed? - Can any information be viewed without being logged in, including after logging off, if so what information?	Yes after 300 seconds. This cannot be changed by the customer as it is set at the system level. No data can be viewed without being logged in.	Noted
<b>Deletion of transactions</b>			
3.17	Is it possible to delete a transaction?	Data can be deleted imediatly by the user and will automatically be deleted after 90 days.	Noted
3.18	If so, then how are deletions controlled by the system?	Access to that function is controlled via the users profile, role based access control privileges	Noted
3.19	Are deleted transactions retained in the audit trail (see below) and denoted as such?	Data can be deleted imediatly by the user and will automatically be deleted after 90 days.	Noted
<b>Audit trails</b>			
3.20	Does the system have an audit trail (log) which records all changes to transactions in the system?	There is a audit trail of changes to the record. The audit log is removed along with the transaction after 90 days	Noted; this is not accessible to the end user.
3.21	Does this log also record any system error messages and/or any security violations?	A separate system log is maintained containing all system generated error messages	Noted
3.22	Is it possible to turn off or delete the audit trail?	No	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
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?	All records generated within the system are indexed with a unique system generated id	Noted
3.24	Are all master file changes recorded in the audit trail?	The concept of a 'master file' is not applicable to this system	-
<b>Compliance</b>			
3.25	Does the system operate in a way that is compliant with data protection legislation including GDPR? How does the system facilitate this?	Before any PII data is captured by the system, the user must provide explicit positive consent for the data to be captured and processed for the purposes of ID&V verification. The privacy policy is provided to the user before consent is requested. The system only retains PII data for the purpose for which consent was given. Under 'right to be forgotten' an individuals PII data can be anonymised (audit and validation result data is retained for audit purposes)	Noted. The GDPR policy is contained within Tiller's Privacy Policy. This will be published to the Verify by Tiller website once it has completed Tiller's Change Management release process; which is currently underway.
3.26	Describe your use of sub-processors if any?	sub-processors are used for 4 key purposes: 1) Cloud Service Hosting (Azure) 2) ID Document validity verification 3) Residential Address Verification 4) PEP & Sanction Screening With the exception Cloud Service Hosting, PII Data is only temporarily shared with sub-processors to verify the individuals details. For those sub-processors no PII data is retained.	Noted
<b>Backup and recovery</b>			
3.27	Is there a clear indication in the software or manuals as to how the data is backed-up and recovered?	This information is available to customers in the system documentation provided	Noted
3.28	How often are backups taken and to what point can restores be done?	All persistent data is backed-up automatically using the following backup schedule and retention policies: Short Term Retention uses Point-in-time restore (PITR) overing the previous 35 days. This allows recovery to any point within the last 35 days.. Long Term Retention uses the following differential backup rotational schedule: Daily every 24 hours Weekly for last 5 weeks Monthly for the last 12 months Annual for the last 5 years	Noted. Backups are for DR purposes of the platform itself.
3.29	How does the software facilitate recovery procedures in the event of software failure? (E.g. roll back to the last completed transaction).	DB level commit control is enforced ensuring records are not committed, and automatically rolled back in the event of a failure	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?	n/a, there is no batch data input facility	Noted
3.31	What features are available within the software to help track down processing problems?	System log is maintained containing all system generated error messages	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
4.	<b>DATA PROCESSING AND REPORTING</b>		
<b>Input and validation of transactions</b>			
4.01	Is data input controlled by self-explanatory menu options?	Yes	Confirmed
4.02	Are these menus user/role-specific?	Yes	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. Data which is allowed to be changed by users is accessible via the operations portal screens.	Noted
4.04	Does the software provide input validation checks such as: - [account] code validation? - reasonableness limits? - validity checks?	All capture fields either within the Operations Portal or the Customer App are validated, dependent on the field type/purpose, for acceptable format & content	Noted
4.05	What control features are within the software to ensure completeness and accuracy of data input?	All mandatory fields enforce completion before data can be saved. Data accuracy is enforced through field level validation, dependent on the field type/purpose, for acceptable format & content	Noted
4.06	How does the software ensure uniqueness of the input transactions? (i.e. to avoid duplicate transactions)	Where applicable such data is validated by the API against stored persistent data in the database	Noted
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, Data is validated within the client browser app	Noted
4.08	Is data input by users validated by routines running on the server before data files are updated?	Yes, in addition to the browser app validation, data is also validated within the service API's	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, reasonableness limits and format constraints are enforced	Noted
4.10	Are responses to erroneous data input clear so that they do not lead to inappropriate actions?	Yes, all validation error messages are clear and informative	Confirmed
4.11	Does the software have an automatic facility to correct/reverse/delete transactions?	Verify is not a transaction based system. However, data is not applied unless it has met the validation rules. Data once written can only be changed if allowed by the current customer journey workflow status. All mandates and individuals are automatically deleted 90 days after their creation to prevent unnecessary personal data retention	Noted
4.12	If yes, are these logged in the audit trail?	n/a	-
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, before any insertion is committed, all data being committed must meet the validation rules or the data cannot be inserted.	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
<b>Import and export of data</b>			
4.15	Can files/attachments be uploaded and stored against any transaction?	No	Noted
4.16	Is there an additional charge made for storage of uploaded files? - If yes, please indicate the cost.	n/a	Noted
4.17	Can data be imported into the system from multiple types of files, e.g. XLS, text, CSV?	Currently no, however import formats (JSON, XML, CSV etc.) are planned to be included in future releases.	Noted
4.18	Explain how the system validates imports into the system and what happens to any import which fails?	n/a	-
4.19	Are imported /interfaced transactions detailed in the audit trail? [See also 3.27]	n/a	-
4.20	Can data be exported from all areas of the system to multiple formats e.g. XLS, CSV, PDF, text; if so specify which formats are supported?	A PDF report containing all capture data and results of the ID and Address Verification and PEP/Sanction screening is generated for each customer in PDF format. We are planning to increase the export formats to include additional formats (JSON, CSV etc).	Confirmed
<b>Data processing</b>			
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)?	Yes, All onscreen function execution validation prevents steps being taken out-of-sequence or if the user has insufficient access rights	Confirmed



Ref	Requirement	Vendor Response	Reviewer Comments
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, however records within the system can be archived or deleted in accordance with Data Retention policies and 'right to be forgotten'	-
4.25	What is the size and format of reference numbers and descriptions within:- - Ledgers? - Stock? - Currencies?	n/a	-
4.26	How does the software guard against/warn about duplicate account numbers on set up?	n/a	-
4.27	How does the software enable the traceability [from, to and through the accounting records] of any source document or interfaced transaction?	There are no accounting records, however all action initiated within the system are written to an Audit log	-
4.28	What drill down/around functionality is available within the software?	There are no accounting records, however users can drill down into the verification results to see the details supporting those results	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	-
<b>Report writer</b>			
4.30	Does the system have an in-built report generator or is a third-party solution used (if so please specify)?	No	Noted
4.31	Is the report writer based on a standard SQL-type approach and is it flexible and easy to use?	n/a	-
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?	n/a	-
4.35	Can users create their own reports? If so, what are the controls on users doing this?	n/a	-
4.36	Can users create saved searches /filters / queries?	n/a	-
4.37	Can regular reports be added to user menus in the appropriate area of the system?	n/a	-
4.38	Does the system support the production of on demand (interactive) and scheduled batch reports?	Yes, on demand: Verification results report	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
5.	<b>USABILITY</b>		
<b>Ease of use</b>			
5.01	Does the solution provide a multi-language user interface?	No, English-only currently. It has been designed to be able to be multi-lingual in future.	Confirmed
5.02	Does the system allow for customizable branding and UI (e.g. corporate colour palate, upload company logo, etc)?	Limited self-serve branding of the iOS and Android mobile app (Company Name and Logo)	Confirmed
5.03	Does the system have a similar look and feel and overall and consistency between screens and modules?	Yes, a single design UX & UI is implemented throughout the application	Confirmed
5.04	Is data entry easily repeated if similar to previous entry?	All user input fields are intuitive with supportive data validation, dropdown lists and informative error messages. Previous entry data is not persisted in fields to ensure data capture accuracy and avoid incorrect data capture	Noted
5.05	Does the software prevent access to a record while it is being updated?	Yes	Noted
5.06	Is there locking at file or record level?	Yes at record level	Noted
5.07	Does the software allow for the running of reports whilst records are being updated?	The validation report is only available after all processing is complete	Noted
5.08	Can timestamps or user comments be added to transactions?	Yes, timestamped comments can be added, these are included in the exported report	Noted
5.09	Is there the ability to store preferences and default values on a per-user basis. e.g. department/team/user?	Not currently but this enhancement is planned for 2023	Noted
5.10	Does the system have the ability to provide user-defined fields with associated validation of data input?	No as this is not required for the service the system is providing	Noted
5.11	Can the system provide users with reminders and notifications e.g. workflows?	Not currently but this enhancement is planned for 2023	Noted
5.12	If the system provides workflows, does it have functionality to substitute/delegate authorisations?	Yes, a mandate can be assigned (delegated) to an user	Noted
5.13	Is there the ability for users to define and configure layouts of letters and forms?	n/a	Noted
5.14	Can users save the parameters of searches?	No	Noted
5.15	Does the system have a "universal search" option, allowing a search to be undertaken over all modules of the system?	No as this is not required for the service the system is providing	Noted
5.16	Can the system store menu option 'favourites' on a per user basis?	No	Noted
5.17	Can a user open multiple windows accessing the same or different modules of the system?	Yes	Confirmed
5.18	Can more than one software function be performed concurrently?	No as this is not required for the service the system is providing	Noted
<b>User documentation and training</b>			
5.19	Is the manual provided as: - hard copy - on CD - by download - via a web-interface?	A help and guidance document will be proved to clients as part of the sign-up process.	Noted
5.20	Does the manual include: - An index or search facility? - A guide to basic functions of the software? - Pictures of screens and layouts? - Examples? - A tutorial section? - Details of any error messages and their meanings?	The help and guidance document will contain instructions and examples of how to use each feature in the Client Portal, including the resulting actions that will occur and any exceptions that may be generated.	Noted
5.21	Is context-sensitive help available within the system?	Yes, some functions and fields provide tool-tips	Noted
5.22	Is the manual and/or help editable by the user (subject to the permissions matrix)?	No	Noted
5.23	Will the Software House make the detailed program documentation (e.g. file definitions for third party links) available to the user, either directly or by deposit with a third party (ESCROW)?	No, This is a subscription service and all system code, DB schemas and documentation remain the sole property of Tiller Group	Noted and not unusual for this sort of system.
5.24	Please detail the training options available?	Online VC based user training is provided to key customer staff as part of the customer set-up process. Additional training can be provided on a T&M basis if requested	Noted
5.25	Who provides training: - Software House? - VAR?	Tiller Technologies Limited	Noted
<b>Support and maintenance</b>			

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?	SaaS (Software as a Service) subscription model charged on a per Individual Verification transaction basis We do not support VAR reseller model	Noted
5.27	How is the product supported: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	Managed service supported by Tiller	Noted
5.28	Do VARs have to go through an accreditation process?	n/a	-
5.29	Is the software sold based upon number of named users or a number of concurrent users?	per Verification Transaction	Noted
5.30	The supplier should detail the support cover options available, covering: - The hours provided? - Associated costs? - The global regions covered?	Tiller Technologies Limited maintains a Support Desk during normal business hours. The Support Desk is staffed between 9am-5pm UK time Monday to Friday (Excluding UK public holidays) and consists of level 1 support via email. Issues escalated to Level 2 and Level 3 support follow the hours stated in the customer SLA agreement. Support is included in the subscription transaction cost	Noted
5.31	Detail the process by which customers raise support requests and how these can be viewed/managed?	Issues are raised via email to our support desk which will issue a unique tracking number for the issue. Management of and current status updates are via email.	Noted
5.32	Please note the methods of support available: - Telephone? - Internet chat? - Remote access to customer workstation? - Other, please specify?	Email, Telephone (UK Business Hours)	Noted
5.33	Do you offer service credits for failure to meet performance around SLA and uptime (if applicable)	Charges are based on a per Individual Verification transaction. Failure to execute/complete a Verification transaction are not charged. However transactions which are completed, regardless of whether the verification was successful or not are charged.	Noted
5.34	What is your escalation path for tickets which have not been resolved within a reasonable time?	Issues initially go to Level 1 support. If issues cannot be resolved by Level 1 the Issues escalated to Level 2 and Level 3 support follow the hours stated in the customer SLA agreement. Escalation of issues and response times are based on our Issue Escalation Policy. Issues are assessed against a matrix of based on their Impact and Urgency. The resulting Severity determines the target resolution times. The target resolution/mitigation time for priority 1 is 2 hours, priority 2 is 4 hours, priority 3 is 14 hours, priority 4 is 24 hours, and priority 5 is 48 hours.	Noted
5.35	How often are general software enhancements provided?	Quarterly	Noted
5.36	Will they be given free of charge?	Yes, unless they were specifically provided at the request of a customer in which case there may be a development/supplementary transaction charge	Noted
5.37	How are enhancements and bug fixes provided to customers?	This is a managed online services so all enhancements and bug fixes are applied by Tiller to the online platform	Noted
5.38	Is "hot line" support to assist with immediate problem solving available?	Yes, there is a support number for urgent client-firm queries, in addition to email.	Noted
5.39	If so, is there an additional cost involved?	No	Noted
5.40	At what times will this support be available?	UK business hours.	Noted
<b>Integration and www facilities</b>			
5.41	Can the software be linked to other packages e.g. word processing, graphics, financial modelling, to provide alternative display and reporting facilities?	No	Noted
5.42	Can definable links to spreadsheets be created?	No	Noted
5.43	Does the system provide a secure document storage capability: If so, please give examples of the document types saved and what transactions these might relate to.	No	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
5.44	Can documents be scanned into a secure repository?	ID Documents, Face Match Images and Secondary Address Verification images are stored securely within the system until deletion (manually or automatically)	Noted
5.45	Does the system provide data migration tools for transactional and master data sets (e.g. employees customers, suppliers, journals, invoices).	No	Noted. Not really applicable.
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?	Data is accessible (Add, Update & Archive) via the Operations Portal. Data is also captured by Individuals being verified via either iOS or Android apps. Direct API access is not available	Noted
5.47	Does the system support mobile working?	Yes, the Operations Portal is accessible via the Internet	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.	<b>SAAS/HOSTED OPERATION</b>		
	<b>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.</b>		
<b>Data centres and customer data</b>			
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?	Microsoft Azure Data centres in Dublin (Primary) and Amsterdam (DR)	Noted
6.02	Does the customer get a choice of the jurisdiction in which their data resides?	By default the Microsoft Azure Data centres in Dublin (Primary) and Amsterdam (DR). However if alternate Azure data centre locations are required by the client this can be arranged but would required a dedicated single tenant implementation likely at additional implementation and ongoing additional cost	Noted
6.03	What certification(s) do you or your platform operators hold relating to your data centres and your business operations?	<b>Tiller:</b> Cyber Essentials <b>Microsoft Azure:</b> ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP, and ENS Full details: <a href="https://learn.microsoft.com/en-us/azure/compliance/">https://learn.microsoft.com/en-us/azure/compliance/</a>	Noted
6.04	Do you or your platform operator have an SSAE16 (System and Organization Controls) report available?	<b>Microsoft Azure:</b> SOC 1, SOC 2, SOC3 reports are available <a href="https://servicetrust.microsoft.com/viewpage/SOC">https://servicetrust.microsoft.com/viewpage/SOC</a>	Noted
6.05	What are the physical controls over the:- - Premises? - Fileservers? - Communications equipment?	<b>Microsoft Azure:</b> All systems and services are hosted in Azure whose data centres are fully compliant with the following ISO 27001/27001, SOC1, SOC 2 standards (see below) <a href="https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security">https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security</a>  <a href="https://servicetrust.microsoft.com/">https://servicetrust.microsoft.com/</a>  <b>Tiller:</b> Implement Information Security Management System (ISMS) standard policies and procedures documented in: ISMS-DOC-A11-1 Physical Security Policy ISMS-DOC-05-4 Information Security Policy ISMS-DOC-A13-1 Network Security Policy ISMS-DOC-A13-5 Electronic Messaging Policy	Noted
6.06	Is the space in this/these data centre(s) shared with any other companies?	Microsoft Azure is a public cloud service provider	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?	The 'Verify by Tiller' product is a multi tenant service. Customers share the same app servers with logical tenant/role security to partition customers' data within the core database.	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?	All access is via authenticated token based access control which implements a data and function capability (Scope) at the API level which determines what data is permitted to be accesses regardless of the request given to the API endpoints. Tokens without that scope to access the data or perform the requested action are denied access by the API endpoint	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
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?	All access is via authenticated token based access control which enforces a data and function capability (Scope) at the API level which determines what data is permitted to be accessed regardless of the request given to the API endpoints. Tokens without that scope to access the data or perform the requested action are denied access by the API endpoint	Noted
6.10	How is [Internet] communication traffic monitored to identify potential problems before they happen: - From a performance perspective? - From a security standpoint?	All external communication including web based and API based services are hosted on managed App Servers. From a performance perspective all services are operate under load balancing which continuously monitors server load and automatically scales-out to additional instances of the service if thresholds are exceeded. Insights monitoring is also used to alert of any abnormal or excessive loads, latency or concurrent connections. In regard to security, all service resources are routed via Azure firewall and NSG (network security group) policy rules. In addition we leverage Azures Monitor Network Insights to identify network health issues and Azure Security for threat awareness & detection	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 data is encrypted at rest and in transit. Access to persistent storage is only permitted via API, which incorporate session scope level controls the level and type of data accessible. All data elements are validated within the API to prevent invalid data being submitted.	Noted
6.12	Are communications between the user's computer and the software service encrypted: - User log in data only? - All data exchanged between user client and software service?	All communication between the user and the software service is encrypted. In addition users login credentials are one-way encrypted including a unique random seed to prevent decrypted without the original user password key	Noted
6.13	Is data on your servers encrypted at rest?	Yes using a 256 bit AES encryption algorithm	Noted
6.14	Is a test environment provided to test configuration changes? If so, is there an additional charge for this?	Yes, a sandbox is provided for users, but this does not connect to the back-end systems.. There is no extra charge for this.	Noted
<b>Access to customer data</b>			
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?	The Data Protection Act requires us in relation to our use Azure as our cloud service provider, to mitigate for the following: <b>Implementing retention effectively in the cloud.</b> We ensure that PII data held is only retained in the cloud databases, backups etc. for the period required to perform our services and that data is deleted at the end of that period. <b>Breach response and notification.</b> We have confirmed that our Agreements with Azure ensure their compliance with regulatory obligations for notification and mitigation support in the event of a breach. This is also covered in our ISMS-DOC-A05-3 Cloud Computing Policy. <b>Processing of personal data outside the European Economic Area (EEA).</b> Only Azure resources and storage hosted and maintained within the EEA are used by our service. We currently use Dublin & Amsterdam datacentres <b>Data portability &amp; data ownership.</b> Our Azure agreement (M412 Microsoft Online Agreement Addendum Financial Services) explicitly ensures provision for data export and our services include export to machine readable formats. The addendum also ensures our compliance with FG 16/5 FCA guidance for outsourcing to the cloud. <b>Risk management.</b> Our Azure provider is subject to our Data Protection Impact Assessment	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.16	Are you subject to any legal or regulatory requirements obliging you to retain a copy of customer data?	No, however we are required to retain sufficient details to be able to confirm explicit consent was given by a customer for the processing of their personal data	Noted
6.17	Who will be able to access or see customer data?	Authorised client staff with access rights determined by their profile security role. Authorised technical support staff if required in response to a technical support issue.	Noted
6.18	Explain the procedures to prevent unauthorised access from staff, or contractors, working for the service provider or any other people with access to the service provider's internal systems.	Our access control policy follows the following 4 principles: <b>Defence in Depth:</b> security must not depend upon any single control but be the sum of a number of complementary controls <b>Least Privilege:</b> the default approach taken must be to assume that access is not required, rather than to assume that it is required, rather than to assume that it is <b>Need to Know:</b> access is only granted to the information required to perform a role, and no more <b>Need to Use:</b> users will only be able to access physical and logical facilities required for their role The use of profiles with privileged access rights is managed through our access control procedures which requires access requests to be documented as to its purpose, need and changes made, authorised and subject to review. Access is only allowed for the period required to satisfy the request.	Noted
6.19	Explain the release management procedures in place and the associated segregation of duties ?	Deployment through each environment, both testing and Production is automated via our CI/CD (Continuous Integration / Continuous Delivery) pipeline process. Release between Development and QA environment, and then between QA and Production are only authorised one the Entry/Exit test criteria has been met and this has been approved by the product owner, Development Manager and Test Coordinator.	Noted
6.20	Is there sufficient segregation of duties preventing system developers from accessing and changing live applications and data files?	Yes, system developers only have access to development and quality assurance test environments. No access to Production and DR environments. If access is required in support of a Production incident this must be requested, authorised and tracked in accordance with our access control procedure described above. Access is granted using a separate (support) profile separate from the support staffs standard profile.	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?	Emergency access/change must follow our Incident Management procedures prior to any access being requested. The incident must first be assessed to determine the incident priority/impact. If the rating (High/Extreme) warrants emergency access/change access can be requested. If access is required in support of a Production incident this must be requested, authorised and tracked in accordance with our access control procedure described above. Access is granted using a separate (support) profile separate from the support staffs standard profile. Post incident follow-up is required to ensure any changes are re-tested through the STLC process and committed to the core code base.	Noted
6.22	Is an audit trail always maintained of these emergency changes?	Yes, via the Support Desk ticket and DevOps Change Management Ticket's	Noted
6.23	What procedures are in place when members of staff leave to ensure that their system access is stopped?	On exit of a staff member the 'ISMS-FORM-A07-3 Employee Termination and Change of Employment Checklist' is followed to ensure all user profiles are disabled/deleted	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
<b>Platform and service levels</b>			
6.24	Which databases can be used (Hosted) or are used (SaaS)?	Verify by Tiller uses Microsoft Azure SQL Databases	Noted
6.25	What forms of user authentication are supported e.g. user names, passwords certificates, tokens etc.?	User Name and Password	Noted
6.26	What is the proposed product/service availability percentage?	99.50%	Noted
6.27	What percentage availability has been achieved over the past 12 months?	Information is not available as this is a new service	Noted
6.28	Is a service level agreement ("SLA") offered regarding: - Service availability? - Data recovery?	No, our SLA sets out our service level objectives, but we do not provide a contractual guarantee of availability. Disaster Recovery, forms an intrinsic part of the service level objectives we set out to deliver. All services and data are backed up on a continuous 'Point in Time Recovery' basis allowing recovery back to any point prior to a failure event. This period extends back covering the last 35 days".	Noted
6.29	Is the service available 24x7 or are there downtime periods for maintenance?	Service is available 24/7	Noted
6.30	Is the customer made aware of maintenance periods in advance?	If maintenance is required then notice will be given. Please note that if for system security or integrity reasons urgent maintenance is required it may not be possible to provide notice	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?	Client staff only required a compatible Internet Browser. Customers must install our iOS or Android app on their mobile device in order to complete the customer ID&V process	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?	The Verify iOS and Android app is only available securely via the Apple and Google App/Play stores.	Noted
<b>Platform security</b>			
6.33	What security steps are taken to prevent and detect intrusion attempts?	Azure Firewall threat intelligence-based filtering to alert on and/or block traffic to and from known malicious IP addresses and domains. Azure Security control is used to monitor for any unexpected activity and adaptive network hardening is used to limit traffic to only expected actual traffic patterns	Noted
6.34	Is firewall hardware and software used to protect the live systems from unauthorised access?	Yes, both Azure Firewall and NSG (Network Security Groups) are used	Noted
6.35	Which monitoring software is used to create alerts when intrusion attempts are suspected?	Microsoft Defender for Cloud Security Alerts	Noted
6.36	Are designated staff responsible for receiving and urgently responding to these alerts?	Yes, IT Administrators	Noted
6.37	Have clear procedures been established for identifying and responding to security incidents?	Yes, these are covered in our ISMS-DOC-A16-2 Information Security Incident Response Procedure	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, Azure App Servers and Azure SQL Servers are automatically updated as a managed service by Azure to the latest versions and patch levels. Azure manages patching on two levels, the physical servers and the guest virtual machines (VMs) that run the App Service resources. Both are updated monthly, which aligns to the monthly Microsoft Patch Tuesday schedule	Noted



Ref	Requirement	Vendor Response	Reviewer Comments
6.39	List the procedures and software tools in place to prevent or detect and eliminate interference from malicious code, such as viruses?	Network hardening and monitoring is covered in our ISMS-DOC-A13-1 Network Security Policy. This covers: <ul style="list-style-type: none"> <li>• The classification of the information to be carried across the network and accessed through it</li> <li>• A risk assessment of the potential threats to the network, taking into account any inherent vulnerabilities</li> <li>• The level of trust between the different components or organizations that will be connected</li> <li>• The security controls in place at locations from which the network will be accessed</li> <li>• Security capabilities of existing computers or devices that will be used for access</li> </ul> The above is enforced through Microsoft Defender for Cloud Security, Security posture, regulatory compliance policies automatically reviewed by the system every 24 hours	Noted
6.40	Is a system log maintained by the service provider that details <ul style="list-style-type: none"> <li>- User access?</li> <li>- User activity?</li> <li>- Error messages?</li> <li>- Security violations?</li> </ul>	Yes, Logs are maintained via diagnostic monitoring and AD Monitoring and covers the following: HTTP Logs, App Service Console Logs, App Service Application Logs, Access Audit Logs, IP Security Audit Logs, App Service Platform Logs, Azure SQL Auditing Logs and Azure AD User Management Logs	Noted
6.41	Is this log available to the customer?	This is a managed multi-tenant service so system level security logs are not directly available to end customers. User level activity logs can be made available on request	Noted
6.42	Have there been any successful unauthorised access attempts been made during the last year? If Yes:- <ul style="list-style-type: none"> <li>- What was the effect on the business and users?</li> <li>- What steps are in place to prevent this happening again?</li> </ul>	No	Noted
6.43	Is penetration testing regularly carried out by (please indicate frequency of tests): <ul style="list-style-type: none"> <li>- Staff specialising in this field?</li> <li>- External specialists?</li> </ul>	Yes, the schedule for external specialist PEN testing is annual or as part of any significant or security related update, whichever is the sooner.	Noted
6.44	If penetration testing by a specialist is not performed regularly, please indicate the main procedures in place to identify weaknesses?		-
6.45	Are security procedures regularly reviewed? Please indicate frequency of reviews.	Yes, quarterly inline with our ISMS-DOC-09-1 Process for Monitoring, Measurement, Analysis and Evaluation and ISMS-DOC-09-4 Procedure for Management Reviews process	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.46	What security reporting is provided demonstrating compliance against certification(s) and policy(ies)?	Internally reporting is via the Microsoft Defender for Cloud security posture dashboard. This covers current status of all resources, both healthy and unhealthy. Compliance with regulatory and security policies (ISO 279001-2013 & SOC). Status of any non conformity and recommended actions. Any security related events are reported following the ISMS-DOC-A16-1 Information Security Event Assessment Procedure. For example the following would be reported: <ul style="list-style-type: none"> <li>• Notification of a change of an admin password</li> <li>• Login and logout information at an unusual time</li> <li>• An unrecognized device having joined the network</li> <li>• Poor performance of a website</li> <li>• A device detected as being down when it should be up</li> <li>• A threshold is breached (or nears being breached) e.g. disk space capacity</li> <li>• Messages from security software e.g. Host-based intrusion detection systems (HIDS)</li> <li>• Unauthorised logon attempts to key servers or domains</li> <li>• Failover devices becoming active</li> </ul>	Noted
6.47	Are any security breaches communicated to customers?	Inline with our ISMS-DOC-A16-2 Information Security Incident Response Procedure and ISMS-DOC-A16-6 Incident Response Plan Data Breach as well as the service contract SLA and security or data breaches will be reported to customers as early as possible but no later than 72 hours of becoming aware of the incident	Noted
<b>Backups by the service provider</b>			
6.48	In relation to backups undertaken by the system provider please explain: <ul style="list-style-type: none"> <li>- How is a customer's data backed up?</li> <li>- How often is this undertaken?</li> <li>- What is backed up?</li> <li>- What's the media used?</li> <li>- Where are backups stored?</li> <li>- How many copies are there?</li> <li>- How long are they retained for?</li> <li>- Who has access to them?</li> <li>- Is the data encrypted?</li> </ul>	All persistent data is backed-up automatically using the following backup schedule and retention policies: <p>Short Term Retention uses Point-in-time restore (PITR) overing the previous 35 days. This allows recovery to any point within the last 35 days..</p> <p>Long Term Retention uses the following differential backup rotational schedule:</p> <p>Daily every 24 hours</p> <p>Weekly for last 5 weeks</p> <p>Monthly for the last 12 months</p> <p>Annual for the last 5 years</p> <p>Backup data is encrypted</p> <p>Backups are only available to administrators after requesting/approved elevated privilege</p>	Noted
6.49	How frequently is a test-restore of backups undertaken?	Every 6 months	Noted
6.50	Can the provider restore from a backups that it has taken at a customer request?	No, This is a multi-Tennent managed service	Noted
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	-
<b>Platform recovery</b>			
6.53	What contingency plans are in place to enable a quick recovery from: <ul style="list-style-type: none"> <li>- Database or application software corruption?</li> <li>- Hardware failure or theft?</li> <li>- Fire, flood and other disasters?</li> <li>- Communication failures?</li> </ul>	Azure datacentres are tier 3 centres providing multipole levels of infrastructure redundancy covering, power, cooling, communications, network connectivity and internal infrastructure providing 99.982% expected uptime. At an application level Tiller implements a geo-redundant infrastructure architecture with servers mirrored between our primary (Dublin) and DR (Amsterdam) datacentres.	Noted
6.54	How often are these plans tested?	Every 6 months	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
6.55	How often are these plans reviewed and updated?	Quarterly, or as part of any significant application update, whichever is the sooner inline with our ISMS-DOC-09-1 Process for Monitoring, Measurement, Analysis and Evaluation and ISMS-DOC-09-4 Procedure for Management Reviews process	Noted
6.56	What are your: - Recovery Point Object (RPO) standards? - Recovery Time Objective (RTO) minimum standards?	RPO: 10 mins RTO: 12 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 data/time stamps within the application are stored in UTC	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?	Inline with FG 16/5 FCA guidance for outsourcing to the cloud and our service contract, should Tiller discontinue the service for any reason all DB data will be exported in delimited file format along with all database schema structures. If the customer terminates their contract the customer data can also be exported, however this will be at the customers expense	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?	Inline with FG 16/5 FCA guidance for outsourcing to the cloud, our contract with Azure (M412 Microsoft Online Agreement Addendum Financial Services) ensures provision for data export and our services include export to machine readable formats.	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, our staffing and training practices endeavour to minimise 'Key Person Risk'	Noted
<b>Platform change management</b>			
6.61	Describe your approach to upgrades including what option customers have not to take upgrades (if any)?	Verify by Tiller is upgraded on a regular cycle with monthly minor updates and quarterly major updates. There is no option for the customer not to take an upgrade	Noted
6.62	Are users able to test the application before new versions go into live use?	No	Noted
6.63	Are users given notice before application changes are applied to the live system?	Yes	Noted
6.64	Are changes delivered into the live environment "switched off" to enable users to test them before enabling them for their environment?	This depends on the change being delivered. Where a new feature is optional for the user then this will be configured off by default.	Noted
6.65	Describe what testing and QA processes are undertaken before upgrades and other changes are made live/available to customers?	Tiller implements a full STLC (Software Testing Life Cycle) approach at each stage of the delivery process. STLC phases are: Requirement Analysis, Test Planning, Test case development, Test setup Test Execution, Test Cycle closure. Test Planning and development covers: Unit, Functional, Security, Performance and Regression testing.	Noted
6.66	If a hosted system, explain the release management procedures in place and the associated segregation of duties?	Deployment through each environment, both testing and Production is automated via our CI/CD (Continuous Integration / Continuous Delivery) pipeline process. Release between Development and QA environment, and then between QA and Production are only authorised one the Entry/Exit test criteria has been met and this has been approved by the product owner, Development Manager and Test Coordinator.	Noted
6.67	Are users informed when they next login of the application changes that have gone into live use?	Release status and release notes are sent via email to each clients contact user. The client is responsible for distributing this information to their staff in accordance with their own user communication policy.	Noted
6.68	Do customer staff have to take any action (e.g. regression testing) when new editions, patches or upgrades are released? If so, please describe what they should ordinarily do.	No	Noted
<b>Subscription options</b>			

Ref	Requirement	Vendor Response	Reviewer Comments
6.69	What is the minimum level of commitment must the customer sign up to, e.g. 36 months?	There is no minimum commitment. The service is sold as Pay As You Go. There is no sign up fee, no minimum usage, no minimum term.	Noted
6.70	Where online payment is used, what type of security is used to protect sensitive information?	N/A - Current invoicing and payment process is via monthly invoicing, with payment accepted via bank transfer.	-
6.71	Where online subscription / payment is used, is an invoice provided to the customer and, if so, in what format?	N/A - Current invoicing and payment process is via monthly invoicing, which is issued as a pdf invoice and sent out via our accounting software.	-
6.72	When subscriptions need to be renewed, what advance notice is provided and what is the time limit for renewal?	N/A this is a PAYG service, with no subscription necessary	Noted
6.73	Is there a procedure for late renewal and is there a time limit after which subscriptions cannot be renewed?	N/A	-
6.74	How soon after creating or renewing a subscription (if applicable) can the system / service be used?	N/A	-
6.75	What notifications / confirmations are provided to the customer regarding subscriptions and payments?	We do not currently send out notifications for payment received.	Noted
6.76	To what extent are users able to access their accounting and other data if: - They miss one or two payments? - They cease being customers?	As there is no subscription, users are no cut off from their account, unless they ask to be removed.	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?	As per 6.76, there is no contract, therefore their account remains open until cancelled by the user. Verify is designed as a 'check & forget' service, so once the information on the customer has been checked by the client, that information is then downloaded to the client. Customer data is automatically deleted after the client has downloaded their customer record in pdf format.	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?	There is no contract, and customer data is automatically deleted, once the customer report is downloaded from the system.	Noted
6.79	What is your processes regarding disposal of end-of-life and failed hardware devices that were used to operate your service?	All resources used to provide the Tiller managed service are run on virtualised hardware within the Azure datacentre. Any data bearing resources which are removed from service within azure are wiped in accordance with NIST 800-80 standards. <a href="https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security">https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security</a> and <a href="https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final">https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final</a> covering Guidelines for Media Sanitization.	Noted
<b>SaaS/Hosted Reporting</b>			
6.80	Are reports produced from the same software as the financial applications or is separate reporting software used?	There is no financial application. Reports are however generated internally by our software	Confirmed
6.81	Does any application software (i.e. other than a web browser or PDF reader) need to be installed on the user's computer in order to prepare or view the reports?	No	Noted
6.82	What browser versions are support: - On desktop/laptop (PC, Mac, Linux)? - On Tablets? - On mobiles?	For each browser we support the current and previous 2 versions of the software. For security reasons we always recommend only using the most current version. Supported browsers are: Chrome (Windows, macOS, Android, iOS) Edge & Firefox (Windows, Android) Safari (MacOS, iOS)	Noted
6.83	Is access to the reporting facilities and data controlled by the same procedures as access to the main application?	Yes	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	-

Ref	Requirement	Vendor Response	Reviewer Comments
6.85	In what electronic formats are reports produced:- - PDF? - XML? - MS Excel spreadsheet? - CSV file? - As html for viewing in a web browser? - Other, please specify?	PDF currently. In future releases we will offer a choice of PDF, JSON, CSV, XML.	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?	On the users computer/client folders.	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?	n/a	-
6.88	Are communications between the browser and the server encrypted for any report related communications?	Yes, HTTPS TLS v1.2 encryption	Noted
6.89	If reports are produced dynamically each time the user views them can historical reports be reproduced at any time?	No	Noted
6.90	Can reports viewable in a browser be navigated dynamically by users? For example: - Enabling drill down to more detailed information? - Altering which columns and rows of data are displayed. - Choosing time periods? - Specifying selection criteria?	n/a	-
6.91	Can report data be reliably copied and pasted direct from browser viewable reports to an MS Excel spreadsheet retaining any table layout?	n/a	-
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?	IF report download is interrupted then the partial downloaded report would be inaccessible as a PDF	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
<b>7.</b>	<b>DIGITAL CLIENT ONBOARDING</b>		
<b>Global Setup</b>			
	Note that the phrase: "Accountant" has been used for the firm of Accountants having individual users of the software, and "Individual" has been used for the customer of the accounting firm on whom the identity checks are being run.		
7.01	Does the system make use of global lists, e.g.: - Countries? - Postcodes? - Client [business/firm] and/or individual types? - Other, please specify?	-Countries list is based on the ISO 3166 list of countries -Postcode global list is not stored within the system, however for address lookup we use an international address lookup tool which returns the appropriate valid postcode for an address within each country. The customer is also able to define their address via entry of first line of address, etc, rather than starting with postcode. This caters for countries that do not follow a postcode / Zip code structure. -Client and/or individual types is not applicable in the application -Other global lists include gender, document type (used in ID&V	Noted
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 ? - Information that has been uploaded? - Information provided by third-parties? - All authorisations/approvals?	-Changes to standing data is not permitted by the user An audit trail of changes to input or updated client data is captured	Noted. Changes cannot be made to third-party lists. The audit trail is not accessible to the end user. See 3.20
7.03	Does the system support multiple languages?	Currently only English is supported	Noted
7.04	Does the system provide inbuilt workflow functionality?	Yes, the client is guided through the verification journey automatically.	Confirmed
7.05	Does the system allow a user to use multiple devices to support mobile working, e.g. a workstation, phone and/or a tablet?	The client capture journey is supported by native apps on iOS and Android. The operations portal is browser based and can be access from workstations	Confirmed
7.06	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?	For security reasons information captured during the client journey are only saved on completion. This is to ensure client sensitive data is not accessible on the client app from previous sessions. Changes made within the ops portal must be saved manually by the user Changes once made within the ops portal cannot be rolled back.	Confirmed
7.07	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): - Providers of identity checking services? - Providers of PEP/Sanctions lists? - Credit check agencies? - Providers of DBS checks? - Banks and other financial institutions? - Others, please specify?	- Providers of identity checking services - YES - Providers of PEP/Sanctions lists - YES - Credit check agencies - YES (Only to verify residential address - no credit check is performed) - Providers of DBS checks - NO - Banks and other financial institutions - NO (Back account verification is on the roadmap to implement Q2 2023 - and in time will be supplemented via open banking capability	Noted
7.08	Does the system provide a portal or access via a mobile-app to enable the exchange of information between the Accountant and their Client(s), the individual(s)?	The Accountant initiates the verification on an individual(s) by entering minimum basic details such as name and email address into the operations portal. The system then sends an invite to the Individual(s) to download a mobile app to capture their full personal details and perform ID document capture & verification. These details are then automatically checked and presented back to the Accountant via the Operations Portal	Confirmed

Ref	Requirement	Vendor Response	Reviewer Comments
7.09	If yes, please clarify the level of security in relation to: - How authentication is managed? - How 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?	Authentication of the Accountant is via User ID and Password. MFA authentication of the Accountant is scheduled to be supported by Q2 2023 and will use authentication app generated TOTP codes. All UI and interface connections for both the Accountant and Individual are over https Password complexity is enforced as follows: at least 12 characters at least 1 uppercase character (A-Z) at least 1 lowercase character (a-z) at least 1 digit (0-9) at least 1 special character not more than 2 identical characters in a row (e.g., 111 not allowed) Login inactivity timeouts are enforced. Inline with current security best practice recommendations regular password changes are not enforced.	Noted
7.10	Are there any limitations on the Internet Browsers used to access the system? If so, please state which browsers/versions are supported?	The Verification operational portal current versions of Chrome, Edge, Firefox (Chromium browsers) and Safari	Noted
7.11	What Accessibility standards have been adhered to in the design of the portal / mobile-app?	W3C WCAG 2 standards are used for guidance but not formally adhered to.	Noted
7.12	Does the system support single sign-on?	No. Support for SSO is under review for inclusion later in 2023	Noted
<b>Setup of Accountant and User Management</b>			
7.13	Does the system allow for the setup and maintenance of the details of the Accountant using the software and valid users within that organisation?	Each user (Accountant) will have their own user id and password. Only the basic information regarding the user (name, email address and access rights is captured)	Confirmed
7.14	If yes, does the system enable the user to change their own details and change their password?	The user can change their own password	Confirmed
7.15	Does the system provide a permissions matrix so that rights can be set at user and group level?	Permission level are very simple with the only privileged rights available being those to administer the company details. All other users have the same permissions. We plan to provide additional enhancements to this during future upgrades.	Noted
7.16	Does this apply to: - Specific areas of functionality? - Links to third-party systems? - Manually adding/editing transactions? - Authorisations? - Other, please specify?	- Specific areas of functionality? Yes in regard to managing the company configuration - Links to third-party systems? Not applicable - Manually adding/editing transactions? All users have the same edit permissions - Authorisations? Not applicable	Confirmed
7.17	Is it possible to define delegated access?	No. this feature is not required given the use cases for the service	Confirmed
7.18	Can multi-level authorisations be set?	Authorisations do not form part of the required functionality of the system	Confirmed
7.19	Can users be "archived" if they are no longer active within the Accountancy firm? If so: - Is a history of the individuals 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?	Users can either be deleted or set to inactive (effectively the same as archive). If deleted, this cannot be reversed. They can be unarchived. No subscription is required for users.	Confirmed
7.20	Are there restrictions on more than one user at the Accountant working on the same Individual at the same time?	No restriction, the record is not locked. Only additions to the data can be made so no conflicts can offer	Confirmed
7.21	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?	The users security level is not visible to the user as part of their display name. A user would typically only have one profile. If for any reason a separate profile was needed by a user (a separate profile with elevated privileges) then yes, they could sign out and sign in with their other profile.	Confirmed
<b>Setup of Individuals and Verifications</b>			

Ref	Requirement	Vendor Response	Reviewer Comments
7.22	Does the system provide for the setup and maintenance of the general details of the Individual for whom verification is required to be undertaken? If so, does this include: - The individual's name? - Address? - Date and Place of Birth and nationality? - Status and category codes? - Free form notes? - A link to the "verifications" for that individual held within the system? - Other contact information, please specify?	Only the basic details required to initiate the verification invite journey with the individual is captured via the portal. E.g. Name plus email address & phone number to receive the generated invite code via email or SMS. All other data required to perform the verification, such as address, DOB, etc. must be completed by the individual themselves	Confirmed
7.23	Can contact information for an Individual be imported using a standard spreadsheet template? If so, how is this validated?	Currently this feature is not supported but may be added as part of a future enhancement.	Noted
7.24	Can document files be uploaded against a client [to support a verification]? - If yes, what format of files is supported, e.g. PDF?	The mobile app allows a customer to upload a 'library' image of a utility bill. This image can only be uploaded by the individual being verified to support their verification process.	Confirmed
7.25	If documents can be held against individuals, 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?	Images uploaded by the individual or images captured during the ID&V verification process are security stored within the system. - Upload/download documents? They can be downloaded - Mark documents as reviewed and/or approved? The individual as a whole can be flagged as reviewed - Manage document retention (for GDPR compliance)? All records/documents on an individual can be deleted on demand but will be deleted regardless after 90 days.	Noted
7.26	Can an individual be flagged as archived, so that new verifications cannot be undertaken? If so, can an archived individual be unarchived by a user with sufficient security privileges?	A mandate can be marked as archived which will archive all individuals associated with that mandate. Once archived a mandate/individual cannot be unarchived. At the end of the configured period (between 14 to 90 days) the records will be automatically deleted.	Confirmed
7.27	Does the system provide for the setup and maintenance of a new verification for an Individual ? If so, does this include: - The individual's name? - The verification type? - The assigned "user" at the Accountants? - Free form notes? - Other verification information, please specify?	The following setup & Maintenance is provided: - The individual's name? Yes - The verification type? Yes - The assigned "user" at the Accountants? Yes - Free form notes? Yes	Confirmed
7.28	Does the selected verification "type" determine the verification workflow that will be followed, e.g. A "full" verification might include ID, address and credit checks?	The verification type will determine which information will be requested from the individual and what verification checks will be performed. E.g. ID Check, Address Check, PEP & Sanction Check, and in the future Bank Account Check). The system allows for templates, which can be defined by the company, as to which services are used for what type of customer	Noted. In future additional types may be added.
7.29	If so, can the checks required be initiated and logged directly in the system?	Yes, once the type is selected and the invite code sent the remaining capture and verification steps are automatic.	Confirmed
7.30	Does the system allow the individual to use a mobile/tablet device in order to provide (capture/upload) information to the platform as part of the verification process? <b>Also, see 7.10 and 7.11 above.</b>	The individual must use with an iOS or Android Mobile Phone to capture their personal data and ID document checks. Currently tablets are not supported as they cannot read the NFC data stored on Passports.	Confirmed
7.31	Does the system automatically contact the Individual; to request their agreement for verification to take place?	Yes, once the user (accountant) enters the minimum individual contact data (see 7.22) an invite code is automatically sent to the Individual with instructions on how to download the app and start the verification journey.	Confirmed
7.32	If so, is the request sent via: - Email? - SMS? - Other, please specify?	Email (Later in Q1 support for SMS)	Noted



Ref	Requirement	Vendor Response	Reviewer Comments
7.33	If so, does the contact method include a link to enable the individual to: - Access a web-page where details can be entered? - Install a mobile app through which details can be entered?	The email contains instructions on how to download the mobile app for either iOS and Android and contains an Invite code which will allow the individual to start the verification journey on the app.	Confirmed
7.34	Does the system enable completed verifications to be removed from the system (for GDPR purposes)? If yes, can this be initiated by the Accountants, the platform provider, or both parties?	Yes, All Individuals details, documents, images and supporting data can be deleted immediately by the user (Accountant) if require. All Individuals details, documents, images and supporting data will be automatically deleted regardless after 90 days	Noted
<b>Address Checking</b>			
7.35	Does the system provide automated validation of the existence of an Individual's addresses: - in the UK? - In Europe? - Worldwide? - Particular territories, please specify?	There are 2 parts to the address verification process. The first part is that the customer selects their address from a pre-populated global list - which ensures that the address exists. The second part is to verify whether the customer lives at that address (thereby replacing the need for a certified utility bill). Residential Address verification is performed against various regulatory acceptable data sources such as Government agencies, Credit Agencies and Utility Companies. Exact countries support is covered in our contract terms as these may vary, however it includes, 27 countries worldwide including UK - please see attached	Confirmed. This is validation and verification.
7.36	Can the results of a check be saved against the verification record together with the data of the check and originating user ID?	Yes	Confirmed
7.37	Does the system capture an image of the address entered? If so, is this uploaded and held in the system against the verification record?	The address is captured as machine readable data from the Individuals input not as an image. An image is separately captured on a supporting document such as a Utility Bill or Bank Statement which has the address on it but this is not automatically verified. Verification is only performed on the machine readable address data captured	Confirmed
<b>Identity Checking</b>			
7.38	Does the system provide automated <b>identity checking</b> functionality?	Yes.	Confirmed
7.39	If so: - What type of check is provided? - What third-party providers are used? - Is a separate/additional subscription required?	- ID Document image capture and verification - Passport NFC encrypted data capture and verification - Individual face image capture and liveness check - Verification of ID Document extracted Individuals image against face capture image check GBG IDScan is used to support the verification process A separate subscription is not required	Confirmed
7.40	Does the system provide integrated <b>biometric ID</b> verification functionality?	Yes.	Confirmed

Ref	Requirement	Vendor Response	Reviewer Comments
7.41	<p>If so:</p> <ul style="list-style-type: none"> <li>- What type of check is provided?</li> <li>- What comparison is made?</li> <li>- Does the check include "liveness" detection?</li> <li>- What third-party checking providers are used?</li> <li>- Is a separate/additional subscription required?</li> </ul>	<ul style="list-style-type: none"> <li>- What type of check is provided? (As per point 7.30)</li> <li>- What comparison is made?</li> </ul> <p>ID Document are compared to document templates for the specific document and issuer, this also includes tamper checks where possible. Encrypted data stored in Passport NFC is checked for integrity, compared to the OCR'ed data and the data captured and the encrypted digital individuals image is extracted and compared.</p> <ul style="list-style-type: none"> <li>- Does the check include "liveness" detection?</li> </ul> <p>Yes, a full interactive liveness check is performed (involving randomised instructions to move around in front of the camera).</p> <ul style="list-style-type: none"> <li>- What third-party checking providers are used?</li> </ul> <p>GBG IDScan is used to support the verification process.</p> <ul style="list-style-type: none"> <li>- Is a separate/additional subscription required? A separate subscription is not required</li> </ul>	Confirmed
7.42	Is there a time-window within which these checks must be undertaken once the process has been started?	The invite code is valid for 24 hours. A new refresh code can be requested	Noted. The App has a "Resend Code" button.
7.43	Does the system provide functionality to check the identity of an <b>organisation</b> associated to an Individual? If so, does this allow for the identification of the organisation's ownership and who has control?	No. Organisation information capture and/or verification is not supported.	Noted
7.44	Does the system provide an integrated link to Companies House in order to verify UK company details?	No. Organisation information capture and/or verification is not supported.	Noted
7.45	<p>If so:</p> <ul style="list-style-type: none"> <li>- Is the link direct to Companies House or via a third-party provider?</li> <li>- Is a separate/additional subscription required?</li> </ul>	N/A	-
7.46	Does the system provide any third-party links for checking <b>overseas companies</b> ? If so, please provide details	N/A	-
7.47	Does the system provide automated <b>PEP and sanctions</b> checking functionality?	Yes, as a one-time check (ie not continuous monitoring).	Confirmed
7.48	<p>If so:</p> <ul style="list-style-type: none"> <li>- What type of check is provided?</li> <li>- What third-party providers are used?</li> <li>- Is a separate/additional subscription required?</li> </ul>	Checks are performed against OFSI, OFAC, Bureau of International Security & Non-Proliferation Sanctions, Security Council Committees resolutions, EU Sanctions, Defence Trade Controls, plus over 80 Unilateral Sanctions and Regulatory Enforcement Lists. PEP's are screened against a globally collated and updated list of Tier 1, 2, 3 PEPs plus PEPs by association GBG ID3Global. A separate subscription is not required	Noted
7.49	Does the system have the facility to produce documentation on a client that shows: <ul style="list-style-type: none"> <li>- <b>Entity structures</b>?</li> <li>- The ultimate beneficial owners?</li> </ul>	No. Organisation information capture and/or verification is not supported.	Noted
7.50	<p>If so, does this cover:</p> <ul style="list-style-type: none"> <li>- Individuals?</li> <li>- Companies?</li> <li>- Trusts?</li> <li>- Pension Funds?</li> <li>- Sole Trader?</li> <li>- Other entities, please specify?</li> </ul>	N/A	-
7.51	Does the system have a database of pre-verified entities? If so, is this updated by the supplier on a regular basis?	N/A	-
7.52	Is the user able to drill down/across into the entity structure and view the details at each level?	N/A	-
7.53	Can the results of all these checks be saved against the verification record together with the date of the check and originating user ID?	Yes	Confirmed
7.54	Does the system provide an easy way for the user to identify and eliminate false positives? If so, is there a multi-select option for this?	Verification of whether a PEP or Sanction match is a false positive must be performed outside the system	Noted

Ref	Requirement	Vendor Response	Reviewer Comments
<b>Additional Checking</b>			
<u>Supplementary documentation:</u>			
7.55	Does the system have a set of standard requests that can be used to request additional client identification related documents and/or provide authorisation from individuals for information searches? If so, are these: - Email templates? - SMS baed messages? - Other, please specify?	All required information and documents are requested based on the Verification Type selected. No additional ad-hoc information can be requested. Authorisation to perform the searches is obtained at the start of the individuals journey before any information is captured or processed to ensure compliance with GDPR	Confirmed
7.56	Is an audit trail retained of the requests made/sent? If so, does the system provide the facility for an internal approval to be undertaken and recorded against each?	An audit trail is maintained for the duration of the request (90 days). As the application is only designed to verify identity business approval processes related to the information returned must be recorded outside the application	Noted; this is not accessible to the end user.
7.57	Can the system apply rules such that a request for additional documentation is automatically undertaken in specific circumstances, e.g. A particular jurisdiction?	All required information and documents are requested based on the Verification Type selected. No additional ad-hoc information can be requested.	Confirmed.
7.58	For documents held against verifications, does the system have functionality to manage these, including the ability to: - Upload/download documents? - Mark documents as reviewed and/or approved? - Manage document retention (for GDPR compliance)? - Other, please specify?	- Upload/download documents? Yes they can be downloaded - Mark documents as reviewed and/or approved? No - Manage document retention (for GDPR compliance)? All data can be removed immediately if required, however all data and files will be deleted regardless after 90 days	Confirmed
<u>Bank checks:</u>			
7.59	Does the system have the ability to confirm the details of an Individual's bank account? If so: - Does this apply to UK banks? - Are other territories supported, please specify?	No, This feature is schedule to be added end of Q1 2023. It applies to UK-based banks (including Crown Dependencies). When added it will be able to: - Matches the individual's contact detail? Yes - is active/live/open? Yes	Noted
7.60	Does the system have the ability to check whether the bank account: - Matches the individual's contact detaile? - is active/live/open?	No, This feature is schedule to be added end of Q1 2023. When added it will be able to: - Matches the individual's contact detail? Yes - is active/live/open? Yes	Noted
<u>Other checks:</u>			
7.61	Does the system provide an integrated link to third-party companies providing <b>credit-checking</b> functionality? If so: - Is a separate/additional subscription required?	No	Noted
7.62	Does the system provide an integrated link to third-party companies providing <b>UK DBS (Disclosure and Barring Service) checking</b> functionality? If so: - Is a separate/additional subscription required?	No	Noted
7.63	Are <b>other verifications</b> provided? If so, please describe these.	No	Noted
7.64	Can the results of all these checks be saved against the verification record together with the date of the check and originating user ID?	Yes. All checked are recorded against the individual and date/time stamped	Confirmed
<b>Dashboard</b>			
7.65	Does the system incorporate dashboard functionality such that the current status of individuals and verifications can be presented to the Accountant on a single screen, showing: - Verification type? - Individual's name? - Status/progress of verification, e.g. new, pending, complete? - Whether there are outstanding reminders/actions? - Whether there are associated documents logged in the system? - Other, please detail?	Yes: - Verification type? Yes - Individual's name? Yes - Status/progress of verification, e.g. new, pending, complete? Yes - Whether there are outstanding reminders/actions? Yes - Whether there are associated documents logged in the system? Yes - All personal data captured such as Address, email, phone number, nationality, Country of Birth, All data extracted from the ID Document	Confirmed

Ref	Requirement	Vendor Response	Reviewer Comments
7.66	If so, can the Accountant navigate directly from the dashboard into: - A historic or currently open verification? - Any outstanding reminders/actions? - A view of the company structure and beneficial owners? - Other, please specify?	- A historic or currently open verification? Yes - up to 90 days - Any outstanding reminders/actions? Yes, current status and last activity - A view of the company structure and beneficial owners? n/a	Confirmed
7.67	Is the Accountant able to share the dashboard with the Client? If so, explain how this operates.	No	Noted
<b>Reports</b>			
7.68	Does the system provide a series of inbuilt reports that cover: - The details of a verification for an individual? - Individual sections of a verification? - Lists of verifications and associated individuals? - Details of individual(s)? - Other, describe the reports available.	- The details of a verification for an individual? Yes - Individual sections of a verification? Yes - Lists of verifications and associated individuals? Yes - Details of individual(s)? Yes - All images captured during the verification process? Yes	Confirmed
7.69	Does the system allow drill through from a report into the underlying verification sections/questions?	No, Reports are exported as PDF's	Confirmed
7.70	Are all reports adequately titled and dated? e.g. verification name/reference, Individual name, pages, numbers etc.	Yes	Confirmed
7.71	Do the reports provide totals where applicable?	Not applicable	-
7.72	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	Confirmed
7.73	If so, does the system allow graphics and/or the Accountant's logos to be incorporated in the page formatting?	No	Confirmed
7.74	Can all reports be print previewed?	PDF can be viewed in the browser before printing if required	Confirmed
7.75	Does the reporting functionality have the facility to scroll up and down when output to screen?	Yes as it is output as a PDF	Confirmed
7.76	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.	Reports are generated only as PDFs. Future enhancements due in Q2 2023 will include other formats such as JSON and CSV	Noted
7.77	Explain how a report [or parts of a report] can be published/provided to the Participant.	Reports are exported as a PDF and available to download. They can then be distributed as needed	Noted