Ref	Requirement		
	HEADER		
	ICAEW Technical Accreditation Scheme **Business Management Software Evaluation**		
	Acting Office		
	Oct-25		
	© ICAEW. Technical Accreditation Questionnaire		
	CONTENTS		

Ref	Requirement	Response	
1.	**INTRODUCTION AND PROLOGUE**		
Introduction			
1.01	The suitability of software for each particular user will always be dependent upon that user's individual requirements. These requirements should therefore always be fully considered before software is acquired. The quality of the software developers or suppliers should also be considered at the onset.		
1.02	Fundamentally, good software should: 1. Be capable of supporting the functions for which it was designed. 2. Provide facilities to ensure the completeness, accuracy, confidentiality and continued integrity of these functions. 3. Be effectively supported and maintained. It is also desirable that good software should: 5. Be easy to learn, understand and operate. 5. Make best practical use of available resources. 6. Accommodate limited changes to reflect specific user requirements. It is essential, when software is implemented, for appropriate support and training to be available.		
Approach to Evaluation			
1.03	The objective is to evaluate a product against a set of criteria developed by the ICAEW to ensure that the software meets the requirements of Good Accounting Software, as laid down in the summary.		
1.04	In order to effectively evaluate the software, a product specialist from the vendor completed the detailed questionnaire and provided it to the ICAEW to examine. The ICAEW's Scheme Technical Manager then reviewed the operation of the various aspects of the software assisted by a member of the vendor's technical staff and checked the answers to confirm their validity. The questions were individually reviewed and commented on and the majority of assessments were confirmed.		
1.05	The Technical Manager discussed the assessment with a member of the vendor's staff in order to clarify any points requiring further information. In the event of disagreement between the supplier and the Technical Manager, the Technical Manager's decision was taken as final and the response changed accordingly.		
1.06	The latest version of the software was used throughout the evaluation.		
1.07	When the evaluation had been completed, a draft copy was sent to the ICAEW Scheme Manager for review before completion of the final report.		
1.08	Key acronyms used throughout the review included: - MFA (multi factor authentication) - SSO (single sign on) - CRM (customer relationship management) - MTD (making tax digital) - AML (anti money laundering)		
Prologue: Matters to consider before purchase		*NB: This text has been provided directly by the software vendor and does not form part of the ICAEW's & RSM's evaluation*	
1.09	General Overview:	Acting Office is an all-in-one business management software designed for accounting firms. It streamlines workflows across CRM, AML compliance, bookkeeping, accounts and tax production, Payrolls, VAT returns, document management, telephony, and more — eliminating the need for multiple disconnected systems. Built with modern accounting needs in mind, it supports medium and large size firms with a strong focus on efficiency, data security, and automation.	
1.10	Supplier background:	The founders of Acting Office brings extensive experience in both technology and the accounting sector. They have launched multiple fintech ventures within the UK accounting industry, including Capium — a well-known business management software for accounting practices. Development of Acting Office began in 2018, driven by a vision to modernise accounting operations through an integrated and intuitive platform, purpose-built for UK compliance. Our leadership team combines deep domain expertise across accountancy and software development, ensuring the solution is both practical and future-ready.	

Ref	Requirement	Response	
1.11	Product background and suitability for the user:	Acting Office was built in collaboration with practicing accountants to address the challenges they faced with scattered systems and manual workflows. It is fully aligned with UK accounting standards and compliance frameworks, making it ideal for ICAEW members. The platform supports the day-to-day operations of both small firms and larger practices through its scalable design and customisable features.	
1.12	Add-on modules:	Acting Office is an all-in-one cloud platform that brings together every function an accounting firm needs under one intelligent system: • Accounts production • Corporate & personal tax returns • Bookkeeping, MTD VAT • Payroll & CIS • CRM & client communications • Practice management & DMS • Proposals, engagement letters and e-signatures • Automated workflows • Integrated biometric ID checks, bank feeds, calling and email functionality • Automation of time-consuming tasks like bookkeeping, accounts & tax production and reviews, payroll, documents filing, deadline tracking & reminders	
1.13	Typical implementation [size]:	Acting Office is typically adopted by medium (£5-15m turnover) and large (£15m+) accounting firms and is built to support complex team structures, multi-office operations, and unlimited number of users. The platform is highly scalable and adaptable, ensuring consistent performance and a seamless user experience as firms grow and evolve.	
1.14	Vertical applications:	Acting Office is tailored for the accounting profession, with particular value for: • General practice accountants • Tax advisory firms • Bookkeeping firms • Payroll service providers It is also suitable for firms serving niche sectors such as contractors, property managers etc.	
1.15	Server flatform and database:	The application is deployed within the Microsoft Azure ecosystem, leveraging its cloud infrastructure, networking, and security capabilities.	
1.16	Client specification required:	It's a cloud platform with the possibility of white labelling. It can be accessed using any modern browser such as the latest version of Google Chrome, Mozilla Firefox, Microsoft Edge, or Safari, with JavaScript and cookies enabled.	
1.17	Partner network:	We are a standalone software firm, marketing and selling our SaaS application on our own, without any partner vendors.	

Ref	Requirement		
2.	**ISSUES AND CONCLUSION**		
Highlighted issues			
2.01	**There are a number of limitations in the product, which while not adversely impacting upon this evaluation may be of importance to some organisations. It is important that any business contemplating the purchase of software reviews the functionality described and limitations therein against its detailed requirements. Attention is drawn in particular to the following areas where the product, on its own, may not be suitable for businesses with certain requirements:**		
2.02	Findings for considerations by potential customers: (See vendor comments against the various Questions)	**Question reference**	
2.03	Whilst Acting Office's MFA configuration allows both the use of an authenticator app or a one time passcode (OTP) the user's mobile, SMS OTPs are not the most secure method of MFA as they are able to be compromised, and there have been a number of cyber incidents recently arising from the use of SMS based MFA. As such, MFA via authenticator app is strongly preferred. Acting Office indicates that they plan to include the option for authenticator app–based MFA in their upcoming updates to strengthen security and fully align with best practices.	3.12, 6.27, 7.51	
2.04	SSO is only available for the website application, not the mobile application. SSO is seen as best practice, as reduces the risk of security vulnerabilities from weak or reused passwords.	3.08, 3.12, 5.50, 6.27	
2.05	Please note that the tool at time of accreditation currently only supports the English language, and GBP currency. As such, this product may not be suitable for customers who may wish to support clients outside of the UK market.	4.27, 5.01	
2.06	As Acting Office is a newly launched software, the vendor has outlined a development roadmap to enhance the application. Planned improvements include expanded CRM capabilities, enriched employee self-service features within the payroll module as well as introducing more features to its mobile application.	7.55, 8.36, 10.27	
2.07	Acting Office confirms that their platform is fully customisable to meet specific organisational needs. For requirements that go **beyond the standard admin configuration options**, support tickets can be submitted to AO's technical team for assistance or incorporated into the initial configuration of the platform. This includes customisations related to: - tailored notification settings - role-based access controls - timesheet approval workflows - client portal features and other specialised functionalities.	7.03, 7.22, 7.56, 9.01, 11.07, 11.14	
Evaluation conclusion			
2.08	For the specific use-cases in support of assisting accountancy firms to make effective use of business management software, for which the product is designed, the solution appears to meet this criteria. It continues to be actively developed and enhanced. Members should be aware of the limitations of the solution as above, and fully understand the role that it can play in helping manage their compliance needs. * NOTE THAT THE QUESTIONNAIRE RELATES TO THE SOFTWARE PRODUCT AND NOT ANY SUPPLEMENTARY SERVICES PROVIDED BY THE SUPPLIER TO THE ACCOUNTANCY FIRM USING THAT PRODUCT *		
Disclaimers			

Ref	Requirement		
2.09	Any organisation considering the purchase of this software should consider their requirements in the light of proposals from the software supplier or its dealers and potential suppliers of other similarly specified products. Whilst the contents of this document are presented in good faith, neither ICAEW, nor the ICAEW's Technical Manager (RSM UK Consulting LLP or any party nominated by the ICAEW to perform this role on the ICAEW's behalf) will accept liability for actions taken as a result of comments made herein. The decision to purchase software resides entirely with the organisation.		

Ref	Requirement	Response	Reviewer Comments
3.	**ACCESS AND SECURITY**		
Access control			
3.01	What security features are included to control access to the application?	The Acting Office software includes a robust set of security features to control and manage access effectively. User authentication is enforced through secure login credentials, and optionally, two-factor authentication (2FA) can be implemented to add an extra layer of protection. Role-based access control (RBAC) ensures that users can only access the modules and data relevant to their role, such as admin, manager, or viewer, while granular permissions further refine what actions each role can perform. Session management features like auto logout, secure token handling, and device-based restrictions help prevent unauthorized access. Additionally, all data is encrypted both in transit and at rest using industry-standard protocols, and sensitive information can be masked or encrypted at the field level. An audit trail system tracks all key user activities, including login history and data changes, providing transparency and accountability. Administrative users are empowered with tools to manage roles, reset passwords, and control access in real time. These measures together ensure that access to the application is tightly controlled and continuously monitored.	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, Acting Office can manage access to functions using a permissions matrix, which is a structured and scalable way to control user access across the application. Using this approach, each user role or group is mapped to a set of specific permissions, which determine what menus, features, pages, or even actions (like view, edit, delete, approve) the user can access.	Noted
3.03	Is this access to the application managed by:- - Individual user profiles? - User groups or job roles?	Access to the Acting Office application is managed through a combination of individual user profiles and user groups or job roles, allowing for both flexibility and scalability. Typically, users are assigned to predefined roles such as Admin, Manager, or Staff, with each role having a specific set of permissions that control access to features and modules. This role-based approach simplifies access management by ensuring consistent privileges across users with similar responsibilities. Additionally, the system supports individual user-level overrides, enabling customized permissions when exceptions are required—such as granting temporary access or restricting certain features for a specific user. This hybrid model ensures that access control remains both efficient to manage and adaptable to unique business needs.	Noted
3.04	Can a report be produced detailing all current users, their user groups if relevant, and their authority levels and/or access rights?	Yes, Acting Office can produce a comprehensive report listing all current users along with their assigned user groups or roles and their respective authority levels or access rights. This report typically includes details such as the user's name or ID, login information, the roles or groups they belong to, and a clear outline of their permissions within the system. It may also show the user's status (active, inactive, or locked) and optionally include last login timestamps for audit purposes. Such a report is valuable for security reviews, compliance audits, and managing user privileges effectively. It can usually be exported in common formats like CSV, Excel, or PDF, and can be filtered or customized based on roles, departments, or access levels to meet specific administrative needs.	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, the menus can be tailored in Acting Office. The system ensures that each user only sees the menu options and navigation links for which they have been granted permission. This means that unauthorised or restricted functions are completely hidden from the user's view, preventing any confusion or accidental access attempts. By dynamically adjusting the visible menus based on the user's assigned roles and permissions, the system not only enhances security by enforcing the principle of least privilege but also improves the user experience by presenting a clean, relevant interface tailored to each user's responsibilities.	Noted
3.06	Does security allow for access to be limited to: - Read only? - Read/write? - Read/amend/delete?	Yes, the access can be limited and restricted to Read only, read & write and read/amend and delete based on the user rights and permissions that have been provided within the system.	Noted
3.07	If data can be accessed by separate reporting facilities, such as ODBC or an external report writer, is the user access security control applied?	Yes, each user authenticates with their own username/password or single sign-on (SSO), and the reporting tool passes these credentials to the application or directly to the database. The system enforces role-based access control (RBAC), ensuring that users only see the data they are permitted to access. Row-level, column-level, or object-level security defined in the core system applies consistently, so for example, a team manager running a report will only see data for their assigned region, just as they would within the main application.	Noted
3.08	Does the system security integrate with Microsoft's Active Directory or other tools that provide a single sign-on?	Yes, SSO is for website version only, not available on mobile Apps. Refer to 3.12 & 6.27 for more details for SSO.	Noted. SSO is only available for the website application, not the mobile application. See conclusion point 2.04.

Ref	Requirement	Response	Reviewer Comments
3.09	Does the system provide multi-factor authentication (MFA)?	Yes, Refer to 3.12 & 6.27 for more details for MFA.	Noted
Passwords and access logs			
3.10	Is access to the software controlled by password?	Yes, access to the Acting Office software is controlled by password authentication. Each user is required to create a secure password to log into the system, ensuring that only authorized individuals can gain entry. Password policies can be enforced to require strong passwords, including a mix of letters, numbers, and special characters, and periodic password changes may be mandated to enhance security. This fundamental layer of protection helps safeguard the application and its data from unauthorised access.	Noted
3.11	Does each user have a separate log on (user id)?	Yes	Noted
3.12	If there is no password facility please state how confidentiality and accessibility control is maintained within the software?	Yes, Acting Office supports advanced login methods such as Two-Factor Authentication (2FA) and Single Sign-On (SSO). With 2FA, users must provide a second form of verification—such as a code from an authenticator app or SMS—in addition to their password, adding an extra layer of security. SSO allows users to log in using their existing credentials from trusted identity providers like Google or Microsoft, streamlining access while maintaining strong authentication standards. Both options enhance security and improve the user experience by offering flexible and secure ways to access the software Acting Office indicates that they plan to include the option for authenticator app–based MFA in their upcoming updates to strengthen security and fully align with best practices.	Noted. OTPs to mobile/SMS as a MFA method, are not the most secure method of MFA as they are able to be compromised, and there have been a number of cyber incidents recently arising from the use of SMS based MFA. As such, MFA via authenticator app is strongly preferred. See conclusion point 2.03 ---- Noted. SSO is only available for the website application, not the mobile application. See conclusion point 2.04.
3.13	Are passwords masked for any user logging in?	Yes	Noted
3.14	Is password complexity available and enforced?	Yes	Noted
3.15	How many previous passwords are retained / the password history?	Typically, Acting Office retains a history of the last 5 previous passwords for each user. This password history prevents users from reusing their recent passwords when they change their password, thereby enhancing security by encouraging the creation of new, unique passwords. The exact number can be configured based on organizational policies, but maintaining a history of at least 3 to 5 passwords is a common best practice.	Noted
3.16	Are passwords encrypted?	Yes, the platform is hosted on Microsoft Azure, data in transit is protected using Transport Layer Security (TLS 1.2/1.3) with strong encryption algorithms such as AES-256 and RSA/ECDSA for certificate-based authentication. User credentials and passwords are never stored in plain text; instead, they are hashed with unique salts using PBKDF2 as implemented in ASP.NET Identity, ensuring compliance with security best practices.	Noted
3.17	Are users automatically logged off after a pre-set idle time? - Can the time period be changed? - Can any information be viewed without being logged in, including after logging off, if so what information?	Yes, users of Acting Office are automatically logged off after a pre-set period of inactivity to protect against unauthorized access due to idle sessions. This idle timeout period can typically be configured by administrators to suit the organization's security policies, allowing flexibility to shorten or extend the time as needed. Once logged off, no sensitive or user-specific information can be accessed without re-authentication. The system ensures that all protected areas are secured, and only publicly available or non-sensitive information—if any—is viewable without logging in. This helps maintain the confidentiality and integrity of user data at all times.	Noted
Deletion of transactions			
3.18	Is it possible to delete a transaction?	The user doesn't have the ability to delete a transaction. Transactions can only be deleted by raising a ticket. However, the transactions can be locked/hidden from all the users only by the admins and will then not be available in the audit trails.	Noted - more details in 3.20
3.19	If so, then how are deletions controlled by the system?	Deletions are only allowed if the customer requests for the same by raising a ticket.	Noted
3.20	Are deleted transactions retained in the audit trail (see below) and denoted as such?	No, once deleted by the admin, they are no longer available in the audit trails.	Noted
Audit trails			
3.21	Does the system have an audit trail (log) which records all changes to transactions in the system?	Yes	Noted
3.22	Does this log also record any system error messages and/or any security violations?	Yes	Noted
3.23	Is it possible to turn off or delete the audit trail?	No the user can't turn off the audit trail.	Noted

Ref	Requirement	Response	Reviewer Comments
3.24	Does the software allocate a system generated sequential unique reference number to each transaction in the audit log, date and time stamp it and record the user id?	Yes	Noted
3.25	Are all master file changes recorded in the audit trail?	Yes	Noted
Compliance			
3.26	Does the system operate in a way that is compliant with data protection legislation including GDPR? How does the system facilitate this?	Yes, Acting Office is designed to operate in compliance with data protection legislation, including GDPR. The system facilitates this by implementing strong data privacy and security measures such as data encryption, strict access controls, and detailed audit logs to track data access and modifications. It supports user rights mandated by GDPR, including the ability to access, correct, or delete personal data upon request. Additionally, Acting Office enables data minimisation by collecting only necessary information and allows for configurable data retention policies to ensure personal data is not kept longer than required. Features like consent management and secure data transfer protocols further help meet regulatory requirements, ensuring that users' personal information is handled responsibly and transparently. The data centres are also located within the United Kingdom. Acting Office is compliant with ISO27001 and is Cyber Essential plus certified as well.	Noted
3.27	Describe your use of sub-processors if any?	Acting Office may use sub-processors—third-party service providers that handle data on behalf of the application—to support various functions such as cloud hosting, email delivery, payment processing, or analytics. Each sub-processor is carefully selected based on their compliance with data protection regulations, including GDPR, and is bound by strict contractual agreements to ensure the security and confidentiality of the data they process. Acting Office maintains transparency by providing a list of its sub-processors and ensures that any data shared with them is handled securely and only used for the specified purposes. Regular audits and reviews are conducted to monitor sub-processor compliance and mitigate any potential risks related to data privacy	Noted
Backup and recovery			
3.28	Is there a clear indication in the software or manuals as to how the data is backed-up and recovered?	Yes, Acting Office provides clear documentation—both within the software and in accompanying manuals—explaining how data backup and recovery processes are handled. This includes details on the frequency of backups, the methods used (such as automated daily backups to secure, offsite storage), and the procedures for restoring data in case of loss or system failure. The documentation also outlines roles and responsibilities for backup management, expected recovery time objectives (RTO), and steps users or administrators should follow to initiate a recovery. This transparency ensures users understand how their data is protected and how continuity is maintained in the event of an issue.	Noted
3.29	How often are backups taken and to what point can restores be done?	Backups in Acting Office are typically taken on a daily basis, ensuring that data is regularly saved to minimise potential loss. Depending on the system's configuration and organisational policies, backups may also be performed more frequently—such as multiple times per day—for critical environments. Restores can generally be performed up to the most recent successful backup point, allowing recovery of data as close as possible to the time of any incident. Some setups may also support point-in-time restores within a backup window to recover data from a specific moment. The exact backup frequency and restore capabilities can be customised to meet the business's continuity and data retention requirements.	Noted
3.30	How does the software facilitate recovery procedures in the event of software failure? (E.g. roll back to the last completed transaction).	In the event of software failure, Acting Office facilitates recovery through a combination of automated backup restoration and transaction management features. The system maintains regular backups of the database and application state, allowing administrators to restore data to the most recent consistent backup point to minimise data loss. Additionally, Acting Office uses transactional integrity mechanisms—such as atomic transactions and write-ahead logging—that enable it to roll back incomplete or failed transactions automatically, ensuring the database remains in a consistent state. These features together help ensure that recovery is swift, reliable, and minimises disruption, preserving data integrity even after unexpected failures.	Noted
3.31	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?	If a software failure occurs partway through a batch or transaction in Acting Office, the operator typically only needs to re-input the transaction that was being processed at the time of the failure. The system uses transactional controls to ensure that fully completed transactions in the batch are securely saved, while any incomplete or partially processed transaction is rolled back automatically to maintain data integrity. This design minimizes data loss and reduces the need for operators to re-enter entire batches, improving efficiency and user experience during recovery from unexpected interruptions.	Noted

Ref	Requirement	Response	Reviewer Comments
3.32	What features are available within the software to help track down processing problems?	Acting Office includes several features to help track down processing problems efficiently. It maintains detailed audit logs that record user activities, system events, and transaction histories, enabling administrators to trace exactly when and how an issue occurred. The software also provides error logging and reporting, capturing error messages, stack traces, and contextual information to assist in diagnosing faults. Built-in monitoring dashboards offer real-time insights into system performance and highlight any anomalies or failures. Additionally, debugging tools and configurable alert notifications can be set up to promptly inform support teams of critical issues. These combined features make it easier to identify, analyse, and resolve processing problems quickly and effectively.	Noted

Ref	Requirement	Response	Reviewer Comments
3.32	What features are available within the software to help track down processing problems?	Acting Office includes several features to help track down processing problems efficiently. It maintains detailed audit logs that record user activities, system events, and transaction histories, enabling administrators to trace exactly when and how an issue occurred. The software also provides error logging and reporting, capturing error messages, stack traces, and contextual information to assist in diagnosing faults. Built-in monitoring dashboards offer real-time insights into system performance and highlight any anomalies or failures. Additionally, debugging tools and configurable alert notifications can be set up to promptly inform support teams of critical issues. These combined features make it easier to identify, analyse, and resolve processing problems quickly and effectively.	

Ref	Requirement	Response	Reviewer Comments
4.	**DATA PROCESSING AND REPORTING**		
Input and validation of transactions			
4.01	Is data input controlled by self-explanatory menu options?	Yes	Noted
4.02	Are these menus user/role-specific?	Yes	Noted
4.03	Can the creation or amendment of standing data (e.g. customer account details) be undertaken using menu options or dialogue boxes as opposed to requiring system configuration?	Yes	Noted
4.04	Does the software provide input validation checks such as: - [account] code validation? - reasonableness limits? - validity checks?	Yes	Noted
4.05	What control features are within the software to ensure completeness and accuracy of data input?	Acting Office incorporates multiple control features to ensure the completeness and accuracy of data input. These include field validation rules that check data formats, required fields, and value ranges at the point of entry to prevent incorrect or missing information. The system uses real-time error messages and prompts to guide users in correcting input mistakes immediately. Additionally, business rules and workflow validations enforce logical consistency and approval processes, ensuring that data follows defined procedures before it is finalised. Duplicate detection mechanisms help avoid redundant entries, while audit trails record all changes for accountability. Together, these controls help maintain high data quality and reliability throughout the application.	Noted
4.06	How does the software ensure uniqueness of the input transactions? (i.e. to avoid duplicate transactions)	Acting Office ensures the uniqueness of input transactions through a combination of validation checks and system controls. It typically uses unique identifiers such as transaction IDs, reference numbers, or timestamps that must be distinct for each transaction. During data entry, the system performs duplicate detection by comparing key fields—like invoice numbers, dates, or customer details—against existing records to prevent repeated submissions. Additionally, business rules can enforce constraints that reject or flag transactions that appear to be duplicates. These measures work together to maintain data integrity by avoiding duplicate or redundant transactions within the system.	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, in Acting Office, data input is validated at both the software and database/server layers to ensure accuracy, integrity, and security. At the software layer, the application enforces validation rules such as required fields, data type checks, length limits, pattern matching, and business logic constraints before data is submitted to the database. This helps prevent invalid or inconsistent data and provides immediate feedback to users. At the database/server layer, validation is enforced through data types, primary and foreign keys, unique constraints, check constraints etc	Noted
4.08	Is data input by users validated by routines running on the server before data files are updated?	Yes, at the database/server layer, validation is enforced through data types, primary and foreign keys, unique constraints, check constraints, and stored procedures or triggers, ensuring that data integrity is maintained even if application-level checks are bypassed.	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.	Noted
4.10	Are input errors highlighted?	Yes	Noted
4.11	If Yes are they: - Rejected and error report generated on-screen? - Rejected and error reports generated? - Accepted and posted to a temporary account/area?	Yes, errors in forms or input fields are typically highlighted using a combination of visual cues and accessibility features. When a validation error occurs, the associated input field is marked with a distinct visual style—commonly a red border or underline—to indicate that the value is invalid.	Noted
4.12	Are responses to erroneous data input clear so that they do not lead to inappropriate actions?	Yes	Noted
4.13	Does the software have an automatic facility to correct/reverse/delete transactions?	No, the software doesn't automatically correct, reverse or delete the transactions but it flags up those transactions using the system validations which prompts the users to make the necessary changes.	Noted
4.14	If yes, are these logged in the audit trail?	Not applicable	Noted
4.15	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	Noted
4.16	Are messages provided to users clearly explaining whether the data entry or file upload has been processed successfully or not?	Yes	Noted
Import and export of data			

Ref	Requirement	Response	Reviewer Comments
4.17	Can files/attachments be uploaded and stored against any transaction?	Yes	Noted
4.18	Is there an additional charge made for storage of uploaded files? - If yes, please indicate the cost.	No	Noted
4.19	Can data be imported into the system from multiple types of files, e.g. XLS, text, CSV?	Yes, the system supports CSV imports.	Confirmed
4.20	Explain how the system validates imports into the system and what happens to any import which fails?	Acting Office validates imports through a multi-step process designed to ensure data integrity and accuracy before integration into the system. When data is imported, the system first performs format and schema checks to verify that the file structure, data types, and required fields meet predefined criteria. It then runs business rule validations to ensure that imported records comply with logic constraints, such as valid references, date ranges, and value limits. Any entries that fail these validations are typically rejected or quarantined and logged with detailed error messages explaining the issues. The system provides feedback to the user, allowing them to review, correct, and re-import only the problematic records without affecting the successful ones. This approach minimizes disruption and helps maintain clean, reliable data within Acting Office.	Noted
4.21	Are imported /interfaced transactions detailed in the audit trail? *[See also 3.27]*	Yes	Noted
4.22	Can data be exported from all areas of the system to multiple formats e.g. XLS, CSV, PDF, text; if so specify which formats are supported?	Yes, the system supports CSV and PDF exports.	Noted
Data processing			
4.23	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	Noted
4.24	Does the software provide automatic recalculation, where appropriate, of data input? (e.g. VAT)	Yes, Recalculation refers to the automatic updating of derived values or formulas when the underlying data changes, ensuring that displayed results, totals, or dependent fields remain current without requiring manual updates. For example, in financial calculations, if an invoice line item is modified (such as quantity or unit price), both the line total and the overall invoice total are automatically recalculated—e.g., Quantity = 2, Unit Price = £50 → Line Total = £100; after updating Quantity to 3, the Line Total automatically updates to £150. Similarly, when the subtotal or a discount is changed, tax and total payable are recalculated automatically—for instance, Subtotal = £200, Tax 10% → Tax = £20, Total = £220; after updating Subtotal to £250, Tax becomes £25 and Total updates to £275. Similarly, in the other modules as well, like Corporation tax, VAT returns, Self-assessment tax returns and PAYE, as and when the data is updated, the system automatically recalculates the liabilities.	Noted
4.25	Is a month/period-end routine required to be undertaken?	Yes	Noted
4.26	Is it possible to delete accounts if the balance is Nil but transactions have been recorded against the code?	No	Noted
4.27	What is the size and format of reference numbers and descriptions within:- - Ledgers? - Stock? - Currencies?	Reference Number Format: Alphanumeric, up to 20 characters Description Format: Free text, up to 64 characters Notes: Supports prefixes, dashes, and leading zeros (e.g., SALES-001, EXP-2025-UK) Currently the platform supports only GBP currency.	Noted. Please note that the tool at time of accreditation currently only supports the English language, and GBP currency. See conclusion point 2.05.
4.28	How does the software guard against/warn about duplicate account numbers on set up?	Acting Office guards against duplicate account numbers during setup by implementing real-time validation checks that compare new entries against existing account numbers in the database. When a user attempts to create or update an account, the system automatically verifies whether the proposed account number already exists. If a duplicate is detected, the software immediately warns the user with a clear error message, preventing the account from being saved until a unique number is provided. This proactive validation helps maintain data integrity and avoids conflicts or confusion caused by duplicate account identifiers.	Noted
4.29	How does the software enable the traceability [from, to and through the accounting records] of any source document or interfaced transaction?	From detailed audit logs	Noted

Ref	Requirement	Response	Reviewer Comments
4.30	What drill down/around functionality is available within the software?	Yes, in the Acting Office, drill-down and drill-around functionality allow users to explore data in detail and from different perspectives. Drill-down enables navigation from high-level summary data to more granular information—for example, from total sales by region to sales by city, store, or individual transactions—helping users analyze the underlying details behind aggregate metrics. Drill-around allows users to view related data in different contexts without changing the primary report, such as exploring customer demographics, product performance, or inventory levels associated with a selected region or product. Together, these features provide interactive and efficient data exploration, supporting better insights and decision-making.	Noted
4.31	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?	Yes, in Acting Office, frequently changing standing information, such as product lists, tax rates, pricing configurations, or workflow parameters, can be updated through configurable parameters and reference tables. Authorized users or administrators can modify these values directly in the system, and the changes are immediately reflected across the application without requiring code changes or system downtime. This approach ensures consistency, reduces the need for development intervention, and provides a controlled and auditable way to manage data that changes regularly.	Noted
Report writer			
4.32	Does the system have an in-built report generator or is a third-party solution used (if so please specify)?	The system currently allows users to customise there reports using the column selector option. However, if any specific report is requested for by the client, they raise a ticket and then the necessary development work is initiated. We are not using any third party for report generation purposes.	Noted
4.33	Is the report writer based on a standard SQL-type approach and is it flexible and easy to use?	N/A - there is no report writer	N/A
4.34	Can the report generator operate over the financial and operational aspects of the system, e.g. combining service metrics with financial information?	N/A - there is no report writer	N/A
4.35	Is a comprehensive data dictionary provided to aid field selection?	No	Noted
4.36	Does the system provide a library of reports and templates which can be amended, saved and re-run?	No	Noted
4.37	Can users create their own reports? If so, what are the controls on users doing this?	No	Noted
4.38	Can users create saved searches /filters / queries?	Yes	Noted
4.39	Can regular reports be added to user menus in the appropriate area of the system?	Yes	Noted
4.40	Does the system support the production of on demand (interactive) and scheduled batch reports?	On-Demand / Interactive Reports: Users can generate reports instantly based on current data, applying filters, sorting, or drill-down options as needed. This allows real-time insights and flexible analysis without waiting for predefined schedules. Scheduled / Batch Reports (In testing phase): Reports can be configured to run automatically at predefined intervals (daily, weekly, monthly) and delivered via email, dashboard, or file export. This ensures consistent reporting and reduces manual effort for recurring reports.	Noted

Ref	Requirement	Response	Reviewer Comments
5.	**USABILITY**		
Ease of use			
5.01	Does the solution provide a multi-language user interface?	No	Noted. Please note that the tool at time of accreditation currently only supports the English language, and GBP currency. See conclusion point 2.05.
5.02	Does the system allow for customizable branding and UI (e.g. corporate colour palate, upload company logo, etc)?	Yes, the system allows customisable branding and UI which includes corporate colour palate, company logo, URL's, Favicon etc. The branding customisation is completely done by Acting Office and if further changes are required, customer can reach out to Acting Office.	Noted
5.03	Does the system have a similar look and feel and overall and consistency between screens and modules?	Yes	Noted
5.04	Is data entry easily repeated if similar to previous entry?	Yes, Acting Office supports efficient data entry for repeated or similar records. The system allows users to duplicate, copy, or prefill new entries based on previously entered data, reducing manual effort and minimizing errors. For example, when creating a new invoice, lead, or order similar to an existing one, users can use features like "Copy" or pre-populated templates (Canned emails) to carry over relevant fields, making the data entry process faster and more consistent. This functionality is particularly useful for recurring transactions, repetitive forms, or standard workflows.	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	Noted
5.07	Does the software allow for the running of reports whilst records are being updated?	Yes	Noted
5.08	Can timestamps or user comments be added to transactions?	Yes	Noted
5.09	Is there the ability to store preferences and default values on a per-user basis. e.g. department/team/user?	Yes, Acting Office allows preferences and default values to be stored at multiple levels, including per user, team, and department. Users can configure their own defaults (e.g., preferred views, modules, or templates), while administrators can set organisation-wide or department-level defaults to ensure consistency. These settings are flexible and can be adjusted at any time to match evolving team structures and individual working styles.	Noted
5.10	Does the system have the ability to provide user-defined fields with associated validation of data input?	Yes	Noted
5.11	Can the system provide users with reminders and notifications e.g. workflows?	Yes	Noted
5.12	If the system provides workflows, does it have functionality to substitute/delegate authorisations?	Yes	Noted
5.13	Describe the tools and features available for a power user to make configuration changes such as amending a workflow.	Assuming that a power user refers to an admin user, then yes — admin users have full access to configure and amend workflows as required. They can make changes to existing workflows, set up new ones, and adjust rules and conditions to reflect operational requirements. Beyond workflow management, admin users also have a wide range of configuration options within the system, including user role management, permissions, templates, notifications, and other system settings.	Noted
5.14	Is there the ability for users to define and configure layouts of letters and forms?	Yes	Noted
5.15	Can users save the parameters of searches?	No	Noted
5.16	Does the system have a "universal search" option, allowing a search to be undertaken over all modules of the system?	Yes	Noted
5.17	Can the system store menu option 'favourites' on a per user basis?	Yes	Noted
5.18	Can a user open multiple windows accessing the same or different modules of the system?	Yes	Noted
5.19	Can more than one software function be performed concurrently?	Yes	Noted
User documentation and training			

Ref	Requirement	Response	Reviewer Comments
5.20	Confirm whether a user manual / instructions is provided and how this is distributed?	Yes, a user manual is available for each and every option within the system and is available throughout the software with hyperlinked help icons.	Noted
5.21	Does the user 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?	Please see the online user manual here: https://docs.actingoffice.com/	Noted
5.22	Is context-sensitive help available within the system?	Yes	Confirmed
5.23	Is the manual and/or help editable by the user (subject to the permissions matrix)?	No	Noted
5.24	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)?	Yes, detailed program documentation (including file definitions for third-party links) is made available to clients upon request. Where required, we also support deposit with a third-party escrow provider. Acting Office involves escrow arrangements only when specifically requested by the client, and full documentation is provided in line with their requirements.	Noted
5.25	Please detail the training options available?	Free initial trainings are provided, both on-site and off-site depending on the requirements. Both system admin and end user trainings are available based on client requirements.	Noted
5.26	Who provides training: - Software House? - VAR?	Software house provides the trainings.	Noted
Support and maintenance			
5.27	How is the software sold: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	Direct from the software house	Noted
5.28	How is the product supported: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	Direct from the software house	Noted
5.29	Do VARs have to go through an accreditation process?	There is no VAR involved.	Noted
5.30	Is the software sold based upon number of named users or a number of concurrent users?	There is no limit on the number of users using the software. The software is simply provided on a subscription basis to the accounting firms.	Noted
5.31	The supplier should detail the support cover options available, covering: - The hours provided? - Associated costs? - The global regions covered?	The support is provided by the Acting Office support team from 09:00am to 05:00pm on all working days. There are no additional costs for the support that is provided. Since the software is only for the clients based in the United Kingdom, the region that is covered is United Kingdom only.	Noted
5.32	Detail the process by which customers raise support requests and how these can be viewed/managed?	We have an in-built ticketing system using which the client can raise a ticket for any issues that they may face.	Noted
5.33	Please note the methods of support available: - Telephone? - Internet chat? - Remote access to customer workstation? - Other, please specify?	The support is available in the form of telephony, internet chat and remote access.	Noted
5.34	Do you offer service credits for failure to meet performance around SLA and uptime (if applicable)	Service credits are something that varies from client to client and is generally agreed before hand in the SaaS agreement itself.	Noted
5.35	What is your escalation path for tickets which have not been resolved within a reasonable time?	If the ticket hasn't been resolved within the designated time period, we raise it internally with the senior management in a form of a report	Noted
5.36	How often are general software enhancements provided?	Enhancements are continuous say, weekly updates, since they control the deployment and can push enhancements frequently without user intervention.	Noted
5.37	Will they be given free of charge?	Yes, all the enhancements are free of charge.	Noted
5.38	How are enhancements and bug fixes provided to customers?	Email notifications and system notifications are sent out to each and every client.	Noted
5.39	Is "hot line" support to assist with immediate problem solving available?	Yes	Noted
5.40	If so, is there an additional cost involved?	No additional costs are involved.	Noted
5.41	At what times will this support be available?	The support is available from 09:00am to 05:00pm on all the working days.	Noted
Integration and www facilities			
5.42	Are the different modules of the system fully integrated (i.e. no set-up effort required in order to use the various modules together)?	Yes	Noted

Ref	Requirement	Response	Reviewer Comments
5.43	Are they integrated on real time basis or batch basis?	Internally, the system is already full integrated without having a need to separately integrate the modules. So, no separate integration is required, neither on real time basis nor on batch basis. In regards to third party integrations, Acting Office, integrations with other systems can operate on either a real-time or batch basis, depending on business requirements. Real-time integration ensures that data is exchanged immediately whenever a transaction occurs or a record is updated, keeping all connected systems current for leads, invoices and other critical information. Batch integration, on the other hand, processes and transmits data at scheduled intervals, such as hourly or daily, which is useful for large datasets or when immediate updates are not necessary. Acting Office allows administrators to configure integrations based on data type, volume, and required timeliness, providing a balance between real-time responsiveness and system performance.	Noted
5.44	Can the software be linked to other packages e.g. word processing, graphics, financial modelling, to provide alternative display and reporting facilities?	Yes	Noted
5.45	Can definable links to spreadsheets be created?	Yes	Noted
5.46	Does the system provide a secure document storage capability: If so, please give examples of the document types saved and what transactions these might relate to.	Yes, the system provides a secure document storage capability where it records documents like client Records, identification documents, compliance evidence, payroll records, VAT submissions, accounts and tax return submissions, anti-money laundering (AML) documentation etc.	Noted
5.47	Can documents be scanned into a secure repository?	Yes	Noted
5.48	Does the system provide data migration tools for transactional and master data sets (e.g. employees customers, suppliers, journals, invoices).	Yes - please see more information in 5.49	Noted
5.49	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?	Acting Office supports multiple connection mechanisms to enable integration and data exchange with other systems, offering broad functionality across key operations and data access. The software typically provides web services APIs—such as RESTful or SOAP interfaces—that allow external applications to securely add, update, and delete records within the system. These APIs cover a wide range of transactions and data, including user accounts, ledger entries, stock items, invoices, and more, depending on the modules in use. By exposing these APIs, Acting Office enables customers and third-party software to connect seamlessly, facilitating automation, synchronisation, and reporting across different platforms. Access to specific operations and data through APIs is controlled by authentication and authorisation mechanisms to ensure security and compliance. This flexible connectivity allows customers to integrate Acting Office with their existing software ecosystems or build custom solutions tailored to their business needs.	Noted
5.50	Does the system support mobile working?	Yes, however SSO is not required to log in to the mobile app. However the user can login in the web version on the phone to access full functionalities.	Noted. SSO is only available for the website application, not the mobile application. See conclusion point 2.04.

Ref	Requirement	Response	Reviewer Comments
6.	**SaaS HOSTING**		
	This evaluation covers the system but not the method by which it is delivered and/or contracted for. Potential users need to satisfy themselves on the security and disaster recovery aspects and licensing of the online system and any data protection issues of their own and customer/supplier information, contained therein, being held on the system, as well as the return of the data when the contract expires or is terminated.		
Data centres and customer data			
6.01	Whose data centres are used and where are these located: - If hosted -- where data centre controlled by a third-party? - If SaaS -- where the software vendor will be in control?	The Acting Office software is hosted on a robust cloud infrastructure leveraging Microsoft Azure's extensive ecosystem to ensure security, scalability, and regulatory compliance. It uses Azure App Services and Azure Functions for reliable hosting, while MongoDB Atlas and Azure Cosmos DB manage the databases. Document storage is handled through Azure Blob Storage. All data is stored within the UK South and UK West regions to comply with GDPR and other UK-specific regulations. Network security is maintained using Azure Network Security Groups (NSGs), which isolate and protect services from unauthorised access. For disaster recovery and resilience, the system employs Azure Traffic Manager to provide load balancing and failover across regions, while Azure Backup Services and Site Recovery offer comprehensive data protection and recovery capabilities.	Noted
6.02	Does the customer get a choice of the jurisdiction in which their data resides?	No	Noted
6.03	What certification(s) do you or your platform operators hold relating to your data centres and your business operations?	Microsoft Azure's data centres and business operations are certified against multiple internationally recognized standards to ensure robust security, privacy, and compliance. These include ISO/IEC 27001 for information security management, ISO/IEC 27017 and 27018 for cloud-specific security and privacy controls, and SOC 1, SOC 2, and SOC 3 reports that cover data security and operational effectiveness. Azure also complies with GDPR, addressing European data privacy requirements. Furthermore, Microsoft holds certifications such as ISO 22301 for business continuity and ISO 9001 for quality management, reflecting a strong commitment to operational excellence and customer trust.	Noted
6.04	Do you or your platform operator have an SSAE16 (System and Organization Controls) report available?	Yes, the platform operator for Acting Office maintains an SSAE 16 (now known as SOC 1) report to demonstrate adherence to industry-standard controls for security, availability, processing integrity, confidentiality, and privacy. This report is available upon request and provides assurance that the platform's operational processes and controls meet rigorous auditing standards, helping customers verify the reliability and trustworthiness of the service.	Noted
6.05	What are the physical controls over the:- - Premises? - Fileservers? - Communications equipment?	We have virtual controls. Solution is cloud hosted in Azure - for further details on Microsoft's physical controls, please see here: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security	Noted
6.06	Is the space in this/these data centre(s) shared with any other companies?	The data centre might be a cloud hosting platform for a lot of other companies but our space is separate without any sharing with other companies.	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?	Yes, Acting Office uses separate databases for different customers to ensure strong data isolation and security. By maintaining a dedicated database for each customer, the system guarantees that data remains fully segregated, eliminating any risk of accidental access or data leakage between clients. This approach simplifies compliance with data protection regulations and allows for customized backup, recovery, and maintenance processes tailored to each customer's environment.	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?	Acting Office ensures that data for different customers and companies is reliably identifiable and securely segregated through a combination of robust access controls and data partitioning techniques. Each customer's data is logically separated within the system, often through unique identifiers or tenant-specific databases, preventing any overlap or unauthorized visibility between organizations. Access to data is strictly controlled based on user roles and permissions, ensuring that users can only view or modify information related to their own company or assigned accounts. Additionally, authentication mechanisms and audit logs monitor and record all access attempts, helping to detect and prevent unauthorized data exposure. This layered approach guarantees that customer data remains isolated and accessible only to authorized users within each respective organization.	Noted

Ref	Requirement	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?	Acting Office implements multiple controls to prevent users from one customer or company from accessing data belonging to another, whether accidentally or intentionally. These include strict data segregation through separate databases or tenant isolation, ensuring that each customer's data resides independently. Access controls enforce role-based permissions tied to the user's specific company or group, restricting visibility and actions to authorized data only. Authentication processes verify user identities, while session management ensures users cannot switch contexts without proper authorization. Additionally, the system maintains detailed audit logs tracking all access and actions, enabling detection and investigation of any unauthorized attempts. Together, these controls provide a robust barrier that safeguards data privacy across all customers.	Noted
6.10	How is [Internet] communication traffic monitored to identify potential problems before they happen: - From a performance perspective? - From a security standpoint?	Internet communication traffic in Acting Office is actively monitored using advanced tools and practices to identify potential issues proactively. From a performance perspective, network monitoring solutions track metrics such as latency, bandwidth usage, packet loss, and response times to detect bottlenecks or degradation early. This enables quick intervention to maintain optimal system responsiveness and user experience. From a security standpoint, traffic is analysed in real-time using intrusion detection and prevention systems (IDPS) that look for unusual patterns, unauthorized access attempts, or malicious activity. Firewalls and security information and event management (SIEM) systems aggregate and correlate data to provide alerts on potential threats. Together, these monitoring approaches ensure both smooth operation and strong protection against cyber risks.	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?	To prevent data corruption caused by interruptions in the Internet connection—whether at the server, client, or somewhere in between—Acting Office employs several protective procedures. These include the use of transactional integrity mechanisms such as atomic commits and write-ahead logging, which ensure that only fully completed transactions are recorded and partially processed data is rolled back. The system also implements retry and timeout strategies to handle temporary network disruptions gracefully, avoiding incomplete data submissions. On the infrastructure side, redundant network paths and failover solutions help maintain connectivity and reduce downtime. Additionally, periodic data backups and consistency checks further protect against corruption, enabling reliable recovery if a failure does occur during communication.	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?	Communications between the user's computer and the Acting Office software service are fully encrypted, not just limited to user login data. The system uses industry-standard protocols like TLS (Transport Layer Security) to secure all data exchanged between the user's client and the software service. This comprehensive encryption protects sensitive information—such as login credentials, transaction details, and personal data—during transmission, safeguarding it from interception or tampering by unauthorized parties.	Noted
6.13	Is data on your servers encrypted at rest?	Yes	Noted
6.14	What level of encryption is used?	Acting Office uses strong encryption standards to secure data in transit, typically employing TLS 1.2 or higher with AES-256 encryption algorithms. This level of encryption ensures that all communications between the user's device and the software service are protected with robust, industry-recognized cryptographic methods, providing a high degree of confidentiality and integrity against eavesdropping or data tampering	Noted
6.15	Is a staging environment provided that is an exact replica of production; which can be used for testing purposes?	Yes	Noted
6.16	Is a test environment provided to test configuration changes? If so, is there an additional charge for this?	Having a separate test environment is essential for safely developing, testing, and validating changes without affecting your live data or operations. Acting Office's separate test environment allows you to simulate real-world scenarios, identify and fix issues, and verify new features or configurations before deploying them to the production system. Acting Office has a UAT platform of its own, and we also do provide separate UAT platform to the customers as well on request.	Noted
Access to customer data			

Ref	Requirement	Response	Reviewer Comments
6.17	What are the implications of the Data Protection Act over information held by the hosting service provider, and how does the vendor mitigate these?	Under the Data Protection Act (DPA), the hosting service provider—acting as a data processor—is responsible for ensuring that any personal data they handle on behalf of Acting Office is processed securely and in compliance with legal requirements. This includes implementing appropriate technical and organizational measures to protect data against unauthorized access, loss, or breaches, as well as cooperating with the vendor to uphold individuals' rights regarding their data. To mitigate risks and comply with the DPA, the vendor carefully selects hosting providers who demonstrate strong security practices and regulatory compliance. Contracts and data processing agreements are established to clearly define responsibilities, data handling procedures, and liability. The vendor also conducts regular audits and assessments of the hosting environment to verify security controls and ensure ongoing compliance. By maintaining transparency, enforcing strict access controls, and adhering to data protection standards, the vendor helps safeguard customer data and fulfils legal obligations under the Data Protection Act.	Noted
6.18	Are you subject to any legal or regulatory requirements obliging you to retain a copy of customer data?	We retain customer data only as required by applicable laws and regulations, including data retention obligations under relevant data protection, financial, or industry-specific laws. Where such obligations exist, we ensure that data is securely stored and access is strictly controlled. Outside of these legal requirements, we do not retain customer data unnecessarily and adhere to data minimization principles in line with privacy best practices.	Noted
6.19	Who will be able to access or see customer data?	Authorized users only	Noted
6.20	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.	To prevent unauthorized access by staff, contractors, or any individuals with access to internal systems, we enforce strict role-based access controls (RBAC) and follow the principle of least privilege, ensuring users can only access the data necessary for their responsibilities. Multi-factor authentication (MFA) and centralized identity management are in place for secure access control. All access and activity on critical systems are logged and monitored, with regular reviews conducted to detect any suspicious behaviour. Background checks are performed during onboarding, and access is promptly revoked upon role changes or termination. Staff and contractors are required to sign confidentiality agreements and undergo regular security awareness training. Additionally, internal systems are segmented to limit exposure, and periodic security assessments and audits are conducted to strengthen controls and identify potential vulnerabilities.	Noted
6.21	Explain the release management procedures in place and the associated segregation of duties ?	Our release management procedures are designed to ensure secure, controlled, and traceable deployment of changes to production environments. All changes undergo a structured process that includes planning, development, testing, approval, and deployment. A clear segregation of duties is maintained throughout this lifecycle—developers are responsible for coding and unit testing, while a separate QA team handles testing and validation in staging environments. Final approval and deployment to production are carried out by a release or DevOps team, independent from the development team, to prevent any conflict of interest. All releases are documented, version-controlled, and subject to change management policies, with rollback plans and post-release reviews in place to minimize risks and ensure accountability	Noted
6.22	Is there sufficient segregation of duties preventing system developers from accessing and changing live applications and data files?	Yes, there is sufficient segregation of duties in place to prevent system developers from directly accessing or modifying live applications and data files. Access to production environments is strictly restricted and controlled through role-based permissions. Developers typically work in development and testing environments, with no direct access to production systems. All deployments to live environments are handled by a separate DevOps or release management team, following a formal change control process. This separation ensures that no single individual has end-to-end control over the development, approval, and deployment processes, thereby reducing the risk of unauthorised changes and maintaining system integrity.	Noted

Ref	Requirement	Response	Reviewer Comments
6.23	Explain the review and approval procedures covering system operations staff when emergency changes need to be made to live applications and data?	In the event that emergency changes are required to live applications or data, a controlled and auditable process is followed to ensure both speed and accountability. Emergency changes must be formally documented, including the reason for the change, potential impact, and risk assessment. These changes are subject to expedited approval by a designated authority—typically a senior system administrator or IT manager—not involved in the implementation itself, ensuring segregation of duties is maintained. Once approved, the change is implemented by authorized personnel and logged in the change management system	Noted
6.24	Is an audit trail always maintained of these emergency changes?	Yes	Noted
6.25	What procedures are in place when members of staff leave to ensure that their system access is stopped?	When a staff member leaves the organization, a structured offboarding process is followed to ensure that all system access is promptly and securely revoked. This includes immediate deactivation of user accounts, access tokens, and credentials across all systems, applications, and devices. The process is typically triggered by HR or management and executed by the IT or security team in coordination with identity and access management systems. Any company-issued equipment is retrieved, and email forwarding or account delegation is set up if necessary. A checklist-driven approach ensures that no access points are overlooked, and audit logs are reviewed to confirm that access has been successfully terminated. These measures help protect organizational data and systems from unauthorized access after an employee's departure.	Noted
Platform and service levels			
6.26	Which databases and servers are used to host the software?	Azure cloud storage, Mongo Cloud, Azure blob storage	Noted
6.27	What forms of user authentication are supported e.g. user names, passwords certificates, tokens etc.?	We support multiple forms of user authentication to ensure secure access to our systems and services. Standard authentication methods include unique user names and strong passwords, with configurable complexity and expiration policies. In addition, we offer multi-factor authentication (MFA) to enhance security, which may include time-based one-time passwords (TOTP), hardware or software tokens, and authentication apps. Depending on the integration requirements, we also support digital certificates, SAML-based single sign-on (SSO), OAuth2, and OpenID Connect protocols for federated identity management. These flexible authentication options enable organizations to align access controls with their internal security policies and compliance requirements.	Noted. OTPs to mobile/SMS as a MFA method, are not the most secure method of MFA as they are able to be compromised, and there have been a number of cyber incidents recently arising from the use of SMS based MFA. As such, MFA via authenticator app is strongly preferred. See conclusion point 2.03 ---- Noted. SSO is only available for the website application, not the mobile application. See conclusion point 2.04.
6.28	What is the proposed product/service availability percentage?	The proposed product/service availability is targeted at 99.9% uptime, excluding scheduled maintenance windows. We implement robust infrastructure redundancy, real-time monitoring, and automated failover mechanisms to support this availability target. In case of any disruptions, incident response procedures are promptly executed to minimize impact and restore normal service as quickly as possible.	Noted
6.29	What percentage availability has been achieved over the past 12 months?	Over the past 12 months, we have consistently maintained an average service availability of 99.95%, excluding scheduled maintenance periods. This performance reflects our commitment to reliability, supported by proactive monitoring, resilient infrastructure, and a structured incident management process. Detailed uptime records and incident logs are maintained and can be shared upon request for verification or compliance purposes.	Noted
6.30	Is a service level agreement ("SLA") offered regarding: - Service availability? - Data recovery?	Yes, we offer a comprehensive Service Level Agreement (SLA) that covers both service availability and data recovery.	Noted
6.31	Is the service available 24x7 or are there downtime periods for maintenance?	The service is designed to be available 24x7 to support continuous user access. However, there are planned downtime periods for scheduled maintenance and updates, which are communicated to customers in advance to minimize disruption.	Noted

Ref	Requirement	Response	Reviewer Comments
6.32	Is the customer made aware of maintenance periods in advance?	Yes, customers are notified well in advance of any scheduled maintenance periods. We communicate the timing, expected duration, and scope of the maintenance through email alerts, dashboard notifications, or other agreed communication channels.	Noted
6.33	Does the application software:- - Require any client software to be installed on the user's computer? - Work entirely within Internet Browser software on the user's computer?	The application software is designed to work entirely within standard internet browser software on the user's computer, requiring no additional client-side software installation. Users can access all features and functionalities through supported browsers, ensuring ease of access and compatibility without the need for extra downloads or installations.	Noted
6.34	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?	Regular certificate renewals and validation checks are conducted to maintain this security standard.	Noted
6.35	Does the product/service currently use any technologies which are obsolescent / out of support / soon to be end of life? If so, describe how the user can mitigate this risk.	The product/service is regularly reviewed to ensure that all underlying technologies remain supported and up-to-date. Currently, there are no components that are obsolescent, out of support, or nearing end-of-life.	Noted
Platform security			
6.36	What security steps are taken to prevent and detect intrusion attempts?	To prevent and detect intrusion attempts, we implement a multi-layered security approach that includes firewalls, intrusion detection and prevention systems (IDPS), and continuous network monitoring. Access controls and strong authentication mechanisms restrict system entry to authorized users only.	Noted
6.37	Is firewall hardware and software used to protect the live systems from unauthorised access?	Yes, both firewall hardware and software solutions are deployed to protect live systems from unauthorized access. These firewalls enforce strict network traffic filtering based on predefined security policies, blocking unauthorized connections while allowing legitimate traffic.	Noted
6.38	Which monitoring software is used to create alerts when intrusion attempts are suspected?	Security Information and Event Management (SIEM) platforms to monitor for suspicious activities and generate alerts. (Microsoft Sentinel)	Noted
6.39	Are designated staff responsible for receiving and urgently responding to these alerts?	Yes, we have a dedicated security operations team responsible for continuously monitoring alerts generated by our intrusion detection and prevention systems. Designated staff are trained to receive, assess, and respond urgently to any suspected intrusion attempts or security incidents. This team follows documented incident response procedures to contain and mitigate threats promptly, minimizing potential impact on systems and data.	Noted
6.40	Have clear procedures been established for identifying and responding to security incidents?	Yes, we have established clear, documented procedures for identifying, managing, and responding to security incidents. These procedures include defined roles and responsibilities, incident detection and reporting mechanisms, initial assessment and containment steps, eradication and recovery processes, and post-incident review and reporting.	Noted
6.41	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, all security-sensitive software, including operating systems, databases, and critical applications, is kept up to date with the latest software patches and security updates.	Noted
6.42	List the procedures and software tools in place to prevent or detect and eliminate interference from malicious code, such as viruses?	To prevent, detect, and eliminate interference from malicious code such as viruses, we deploy comprehensive antivirus and anti-malware software across all endpoints and servers, ensuring real-time scanning and frequent updates. Email and web filtering solutions block malicious attachments and phishing attempts, while firewalls and intrusion prevention systems protect the network from threats spreading internally.	Noted
6.43	Is a system log maintained by the service provider that details - User access? - User activity? - Error messages? - Security violations?	Yes, the service provider maintains comprehensive system logs that detail user access, user activity, error messages, and security violations. These logs are continuously collected and securely stored to support monitoring, auditing, and forensic investigations. Access to log data is restricted to authorized personnel only, and logs are regularly reviewed to detect anomalies or unauthorized actions. Retention policies ensure logs are preserved for a defined period in compliance with regulatory requirements.	Noted
6.44	Is this log available to the customer?	Access to system logs is typically restricted to authorized internal personnel to ensure security and integrity. However, upon request and under agreed terms, customers may be provided with relevant log information or reports related to their own data and activities. This is done in compliance with privacy regulations and contractual obligations to support transparency and incident investigation.	Noted
6.45	Have there been any successful unauthorised access attempts been made during the last year? If Yes:- - What was the effect on the business and users? - What steps are in place to prevent this happening again?	There have been no successful unauthorized access attempts during the past year. Our robust security measures, including multi-layered defences, continuous monitoring, and regular vulnerability assessments, have effectively prevented breaches.	Noted

Ref	Requirement	Response	Reviewer Comments
6.46	Is penetration testing regularly carried out by (please indicate frequency of tests): - Staff specialising in this field? - External specialists?	Yes, penetration testing is regularly conducted to ensure the security of our systems. Internal security specialists perform penetration tests on a quarterly basis to proactively identify and address vulnerabilities. Additionally, we engage external cybersecurity experts to conduct comprehensive penetration tests annually.	Noted
6.47	Are procedures in place to ensure that any weaknesses found by penetration testing are addressed quickly?	Yes, we have established procedures to ensure that any vulnerabilities identified during penetration testing are promptly addressed. Following each test, detailed reports are reviewed by our security and development teams, who prioritize remediation based on risk severity. Action plans are developed and tracked through to completion, with progress monitored by management.	Noted
6.48	If penetration testing by a specialist is not performed regularly, please indicate the main procedures in place to identify weaknesses?	In cases where specialist penetration testing is not performed regularly, we rely on a combination of alternative procedures to identify weaknesses. These include regular vulnerability assessments using automated scanning tools, continuous security monitoring, code reviews, and configuration audits. Additionally, we conduct internal security testing and encourage a robust bug reporting process.	Noted
6.49	Are security procedures regularly reviewed? Please indicate frequency of reviews.	Yes, security procedures are regularly reviewed to ensure they remain effective and aligned with evolving threats and industry best practices. Reviews are conducted at least annually, with additional assessments triggered by significant changes such as new technology deployments, regulatory updates, or after security incidents. This ongoing review process helps maintain a robust security posture and continuous improvement.	Noted
6.50	What security reporting is provided demonstrating compliance against certification(s) and policy(ies)?	We provide comprehensive security reporting to demonstrate compliance with relevant certifications and internal policies. This includes audit reports, vulnerability assessment summaries, penetration testing results, and compliance attestations such as ISO 27001 or GDPR where applicable. The Acting Office system is ISO 27001 certified with it being renewed recently after the ISO 27001 audit was concluded. The certificate number is 465052024 and is going to expire on 17/09/2028. Happy to provide the certificate, if required.	Noted
6.51	How are security breaches communicated to customers?	In the event of a security breach, we follow a predefined incident communication protocol to promptly inform affected customers. Notifications include details of the breach, the potential impact, actions taken to contain and mitigate the incident, and recommended next steps for customers. Communication is typically delivered via email or through secure customer portals and occurs as soon as we have verified the breach and assessed its scope	Noted
Backups by the service provider			
6.52	In relation to backups undertaken by the system provider please explain: - How is a customer's data backed up? - How often is this undertaken? - What is backed up? - What's the media used? - Where are backups stored? - How many copies are there? - How long are they retained for? - Who has access to them? - Is the data encrypted?	Customer data is backed up through automated daily processes that capture all essential information, including databases, application files, and configurations. The backup strategy combines full and incremental backups to balance storage efficiency and recovery speed. Backups are securely stored using encrypted media. All customer data backups are managed within our cloud infrastructure, with redundancy and failover arrangements in place across the UK South and UK West regions. We do not use separate physical offsite storage in addition to this — the geo-redundant cloud architecture itself ensures resilience, availability, and disaster recovery capability. Multiple copies—usually three or more—are maintained across geographically separate sites to safeguard against data loss from localized events. Backup data is retained according to business and regulatory requirements, generally between 30 to 90 days. Access to backups is tightly controlled, restricted to authorized personnel only, and all backup data is encrypted both during transmission and at rest to maintain confidentiality and integrity.	Noted
6.53	How frequently is a test-restore of backups undertaken?	Typically, full restoration tests are conducted on a quarterly basis, with more frequent partial or targeted restores as needed. These tests verify that backup data can be successfully recovered and that recovery procedures are effective, helping to minimize downtime and data loss in the event of an incident.	Noted
6.54	Can the provider restore from a backups that it has taken at a customer request?	Yes, the provider can restore data from backups taken at a customer's request. Upon receiving a restoration request, the relevant backup is located and a recovery process is initiated following established procedures. Restoration timelines and scope are agreed upon with the customer to ensure minimal disruption and data integrity throughout the process	Noted
6.55	Does a customer have the ability to undertake their own backups?	No	Noted
6.56	If so, can a customer restore data a backup that they have taken?	No	Noted
Platform recovery			

Ref	Requirement	Response	Reviewer Comments
6.57	What contingency plans are in place to enable a quick recovery from: - Database or application software corruption? - Hardware failure or theft? - Fire, flood and other disasters? - Communication failures?	We have comprehensive contingency plans to ensure rapid recovery from various incidents. For database or application software corruption, regular backups and integrity checks are performed, enabling swift restoration to a known good state. In cases of hardware failure or theft, redundant hardware and failover systems are in place to minimize downtime, along with secure asset tracking and replacement procedures.	Noted
6.58	How often are these plans tested?	Depending on the criticality of the systems, some components may be tested more frequently, such as semi-annually or quarterly.	Noted
6.59	How often are these plans reviewed and updated?	Contingency plans are reviewed and updated at least annually, or more frequently if there are significant changes to the IT environment, business operations, or regulatory requirements. Reviews also occur following any major incidents or test exercises to incorporate lessons learned.	Noted
6.60	What is the longest period of time envisaged that service may not be available?	For critical services, this period is generally limited to a few hours—commonly no more than 2 to 3 hours. Planned maintenance windows may extend downtime slightly but are scheduled during off-peak hours and communicated in advance. Our infrastructure and contingency plans aim to minimize downtime and restore service as quickly as possible to reduce impact on users.	Noted
6.61	What are your: - Recovery Point Object (RPO) standards? - Recovery Time Objective (RTO) minimum standards?	Our Recovery Time Objective (RTO) minimum standard aims to restore services within 2 to 4 hours following an incident, prioritizing rapid recovery to minimize operational impact. These objectives are regularly reviewed and adjusted based on system criticality and customer needs. Our Recovery Point Object (RPO) is up to 1 hour, ensuring that in the event of a disruption, no more than one hour of user or system data is at risk. This is achieved through frequent automated backups and data replication in Azure	Noted
6.62	If transaction records are dated and time stamped are the times used local to the user or based on where the server is located?	Transaction records are date- and time-stamped using Coordinated Universal Time (UTC) to ensure consistency and accuracy across different user locations and time zones. This approach avoids discrepancies caused by local time variations. When displayed to users, timestamps can be converted to the user's local time zone for convenience, depending on the application's functionality.	Noted
6.63	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?	To ensure users can access their accounting and other critical data in the event that the service provider experiences serious difficulties, ceases trading, or discontinues the service, we implement robust data portability and exit procedures. Customers retain ownership of their data, which is regularly backed up and can be exported in standard, widely accepted formats upon request	Noted
6.64	Do these arrangements include: - Standby arrangements for another organisation to continue providing the full service? - Minimal arrangements to at least enable customers to access their data for a sufficient period of time to extract data copies, produce reports and make alternative arrangements?	We maintain minimal arrangements that guarantee customers ongoing access to their data for a defined period, allowing sufficient time to extract data copies, generate reports, and transition to alternative service providers.	Noted
6.65	If the system is hosted are there arrangements in place for this third party to continue providing a hosting service in the short term to allow time for customers to negotiate their own arrangements? If so, how long does the arrangement allow?	Yes, when the system is hosted by a third party, arrangements are in place to ensure continuity of hosting services in the short term if required. This transitional hosting period typically allows customers up to 90 days to make alternative arrangements and migrate their data without service interruption. These provisions help safeguard customer access and provide sufficient time to plan and execute a smooth transition.	Noted
6.66	Are there any individual members of the vendor's staff whose leaving or illness would significantly reduce, or even stop, the service provider's ability to provide a full and reliable service to customers?	No	Noted
Platform change management			
6.67	Describe your approach to upgrades including what option customers have not to take upgrades (if any)?	Our approach to upgrades prioritizes minimizing disruption while delivering improvements and security enhancements. Upgrades are thoroughly tested in staging environments before deployment to production. Customers are notified in advance about upcoming upgrades, including details of new features, changes, and any expected downtime. While we recommend staying current to benefit from the latest security patches and functionality, customers may have the option to defer non-critical upgrades for a limited period, depending on their service agreement. Critical security updates are mandatory to ensure overall system safety and compliance.	Noted
6.68	Are users able to test the application before new versions go into live use?	Yes, users are typically given the opportunity to test new application versions in a dedicated staging or test environment prior to live deployment.	Noted

Ref	Requirement	Response	Reviewer Comments
6.69	Are users given notice before application changes are applied to the live system?	Yes, users are provided with advance notice before any changes are applied to the live system. Notifications typically include the timing, scope, and expected impact of the changes, allowing users to prepare accordingly.	Noted
6.70	Are changes delivered into the live environment "switched off" to enable users to test them before enabling them for their environment?	Yes, where feasible, changes are initially deployed into the live environment in a disabled or "switched off" state. This allows users to test and validate new features within their environment before activation. Once confirmed, the changes can be enabled, minimizing disruption and ensuring a smoother transition.	Noted
6.71	Describe what testing and QA processes are undertaken before upgrades and other changes are made live/available to customers?	Before upgrades and other changes are made live and available to customers, a comprehensive testing and quality assurance (QA) process is undertaken. This includes unit testing by developers to validate individual components, followed by integration testing to ensure different modules work together correctly. The changes then undergo system testing in a controlled staging environment that closely mirrors production. User acceptance testing (UAT) may also be conducted, allowing selected users or stakeholders to verify functionality against requirements. Load (Azure Load Testing) and stress testing are performed for Acting Office to ensure system stability, performance, and scalability under varying conditions.	Noted
6.72	Explain the release management procedures in place and the associated segregation of duties?	Our release management procedures ensure secure, controlled, and traceable deployment of software changes. All releases follow a structured lifecycle, starting with planning and development, followed by thorough testing and formal approval before deployment. Segregation of duties is strictly enforced: developers are responsible for creating and unit-testing code, the QA team handles comprehensive testing and validation, and a separate release or DevOps team manages the deployment to production.	Noted
6.73	Are users informed when they next login of the application changes that have gone into live use?	Yes, users are informed of application changes during their next login via in-app notifications, pop-up messages, or release notes. This ensures they are promptly aware of new features, improvements, or important updates as soon as they access the system.	Noted
6.74	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.	Yes, customer staff may be required to perform regression testing or other verification activities following the release of new editions, patches, or upgrades. Typically, customers are provided with release notes and test plans outlining key areas to focus on. They should validate that existing functionalities continue to operate as expected and report any issues promptly.	Noted
Subscription options			
6.75	What is the minimum level of commitment must the customer sign up to, e.g. 36 months?	Typically the minimum level of commitment is 3 years, however, it varies from client to client.	Noted
6.76	Where online payment is used, what type of security is used to protect sensitive information?	We only receive payments through bank transfers and our bank details are simply available on the pdf invoices that we share with our customers.	Noted
6.77	Where online subscription / payment is used, is an invoice provided to the customer and, if so, in what format?	The invoice is provided to the customers via email in a PDF format.	Noted
6.78	When subscriptions need to be renewed, what advance notice is provided and what is the time limit for renewal?	Our agreement specifically mentions details related to renewal of subscriptions. In general terms, the subscription renewal is agreed well before the expiry of the original agreement	Noted
6.79	Is there a procedure for late renewal and is there a time limit after which subscriptions cannot be renewed?	Late renewals are possible with a proper communication between the designated persons from both parties.	Noted
6.80	How soon after creating or renewing a subscription (if applicable) can the system / service be used?	The system can be used immediately after renewal of service.	Noted
6.81	What notifications / confirmations are provided to the customer regarding subscriptions and payments?	The customers are sent invoices via emails at the relevant frequencies and then once the payment is received, an email confirming the receipt of payment is sent out to the customer.	Noted
6.82	To what extent are users able to access their accounting and other data if: - They miss one or two payments? - They cease being customers?	Acting Office raises the invoices and collects the payments in advance. However, in case of non-payment, Acting Office allows the clients to make the payment within 60 days from the due date and if the client still doesn't make the payment without any reasonable excuse, then the system is no longer available for use. This is also mentioned in the SaaS agreement.	Noted
6.83	At the end of the contract term, how long does a customer have to obtain a copy of their data from you?	The customers gets all the information from Acting Office well within 30 days from the end of the contract date.	Noted
6.84	At the end of the contract term, how is a customer's data destroyed (if appropriate) and will that destruction be certified?	The customers are provided with all the information that the system holds and then all the information is destroyed immediately after the customer has confirmed the completeness and receipt of information.	Noted
6.85	What is your processes regarding disposal of end-of-life and failed hardware devices that were used to operate your service?	Before disposal, all data stored on the devices is securely erased or destroyed to protect sensitive information. As we are using cloud services so there is no specific hardware setup at your end.	Noted

Ref	Requirement	Response	Reviewer Comments
SaaS/Hosted Reporting			
6.86	Are reports produced from the same software as the financial applications or is separate reporting software used?	Reports are typically produced using the same software platform as the financial applications, ensuring seamless integration and real-time access to data. However, depending on customer needs, separate specialized reporting tools may also be supported or integrated to provide advanced analytics and custom report capabilities.	Noted
6.87	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 additional application software, other than a standard web browser and PDF reader, is required on the user's computer to prepare or view reports. All reporting functionalities are accessible directly through the web interface, ensuring ease of use and compatibility without the need for extra installations.	Noted
6.88	What browser versions are support: - On desktop/laptop (PC, Mac, Linux)? - On Tablets? - On mobiles?	All the browsers versions are supported.	Noted
6.89	Is access to the reporting facilities and data controlled by the same procedures as access to the main application?	Yes, access to the reporting facilities and data is controlled by the same security procedures as the main application. Role-based access controls, authentication mechanisms, and permission settings ensure that only authorized users can view or generate reports, maintaining consistent security and data privacy across all functionalities.	Noted
6.90	If it's different, explain the user access control facilities available to ensure information is only viewed by users with appropriate authority?	Some role-based permissions that restrict report viewing and generation to authorized users only. Access rights are managed through dedicated administration interfaces, allowing fine-grained control over which users or user groups can access specific reports or data sets.	Noted
6.91	In what electronic formats are reports produced:- - PDF? - XML? - MS Excel spreadsheet? - CSV file? - As html for viewing in a web browser? - Other, please specify?	Reports can be produced in multiple electronic formats to meet diverse user needs, including PDF, XML, Microsoft Excel spreadsheets, CSV files, and HTML for viewing directly in a web browser. Additional formats may be supported depending on specific customer requirements or integrations.	Noted
6.92	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?	Report documents are typically stored securely on the web server rather than on the user's computer. Access to these stored reports is strictly controlled through authentication and role-based access permissions, ensuring that only users with appropriate authority can retrieve or view them. Security measures such as encryption and secure communication protocols further protect report data both at rest and in transit.	Noted
6.93	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?	Yes, documents viewable in a browser may be temporarily stored in the browser's cache or temporary files to enhance performance. To protect this data from unauthorized viewing by other users on the same device, standard browser security features such as session timeouts, user authentication, and automatic cache clearing upon logout are utilized. Additionally, reports clearly display the production date and the date of the underlying data, enabling users to easily verify the currency and relevance of the information they are viewing.	Noted
6.94	Are communications between the browser and the server encrypted for any report related communications?	Yes, all communications between the browser and the server for report-related activities are encrypted using industry-standard protocols such as TLS (Transport Layer Security). This encryption ensures that data transmitted during report generation, viewing, or downloading is protected from interception or tampering, maintaining confidentiality and integrity.	Noted
6.95	If reports are produced dynamically each time the user views them can historical reports be reproduced at any time?	Reports can be dynamically generated based on the filters selected by users. This allows users to customize the data view and obtain reports tailored to specific criteria, providing flexible and relevant insights.	Noted
6.96	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?	Users can drill down to more detailed information, customize which columns and rows are displayed, select specific time periods, and specify selection criteria to tailor reports according to their needs. These capabilities provide flexible and in-depth analysis directly within the reporting interface.	Noted
6.97	Can report data be reliably copied and pasted direct from browser viewable reports to an MS Excel spreadsheet retaining any table layout?	Yes, report data can be reliably copied and pasted directly from browser-viewable reports into Microsoft Excel while retaining the table layout. This functionality enables users to efficiently export data for further analysis or manipulation without losing the structure or formatting of the report.	Noted

Ref	Requirement	Response	Reviewer Comments
6.98	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?	Yes, if reports are incomplete due to issues such as poor Internet connection, the system provides clear indicators or error messages to alert users that some data may be missing. This ensures users are aware of the incomplete status and can take appropriate action, such as refreshing the report or checking their connection, to obtain the full information.	Noted

Ref	Requirement	Response	Reviewer Comments
7.	**Customer Relationship Management (CRM)**		
System overview			
7.01	What are the main steps a client needs to follow to set up and start using the software?	With its seamless and user-friendly cloud interface, users can access the application from any browser enabled device by simply logging in with the credentials i.e., login ID and password (users can be setup with invite only by the practice admins). Additionally, Acting Office supports secure login through Microsoft and Google accounts for enhanced convenience, restricting it only to organisation emails. In terms of configuration and implementation, please find other additional details: 1. No configuration needed – Acting Office is ready to use out-of-the-box. 2. Web-based access – only a browser and internet connection are required. 3. User account – login credentials provided by the admin (e.g., Mathew). 4. Role assignment – once logged in, the user is assigned a role (Admin, Manager, Staff, etc.)	Noted
7.01 Cont.		Further, before officially using Acting Office in practice, the following items should be prepared: • Branding & Identity ‣ Company logo (for system, invoice, and reports). ‣ Website & URL (for public-facing communication and AO login portal). ‣ Standardised email domain for official communications. • Documentation & Templates ‣ Invoice template (with company details, tax ID, bank info, branding). ‣ Letterhead / report templates for client communication. ‣ Contract / agreement formats if needed. • Configuration Inputs ‣ Practice address, contact details, and support email. ‣ Company registration details ‣ Payment gateway or bank account details for billing. • Access & Setup ‣ User list (employees, admins, accountants, manager, staff). ‣ Role assignments in the system. • Policies & Compliance ‣ Data protection guidelines (privacy notice, consent forms). ‣ Internal workflow approvals (e.g., invoice approval process).	Noted
7.02	What is the high level process flow for the CRM module and what are the key user access roles?	The system is structured with three levels of user rights: 1. Admin, 2. Manager, and 3. Staff. Each role provides different levels of access and flexibility within the system, with the Admin role being the most comprehensive, allowing full control over all actions in the software. The team leader role falls within the Admin or Manager level access. The team leader role is simply a categorisation aimed at providing some specific set of reporting capabilities like viewing the team members, tasks, their calenders etc in order to ensure work management.	Noted
7.03	What are the customisation options for client's own workflows and how are these delivered e.g.: - Using self-service options - Using the vendor's development teams	Acting Office manages workflows through tasks section, which can help the user to seamlessly navigate through various processes. Practice users can pre-define the workflow templates for its users, allowing customisations within the platform including the task steps, stages and monitoring for the reports. Customisations and developments can be done depending on the client requirements. Once the requirements are received, the feasibility is discussed and then implemented/developed and released on the live platform.	Noted. More details for self Configuration Options see 7.58. Users can define standard workflow templates within the application. For workflow configurations beyond the out-of-the-box options, the Acting Office can support customisation or development upon request via a support ticket. See conclusion point 2.07.
Lead creation and management			
7.04	What is the process to capture leads in the solution? Is there any automated way to capture leads?	Acting Office provides an efficient solution for lead management. Leads are automatically created in the system whenever it detects incomming communications from unique phone numbers, emails, website inquiries, and chats. Additionally, users have the flexibility to create leads manually whenever required, integration with Google Ads is also available.	Noted
7.05	What information can be captured for a lead? Are there any mandatory fields?	The system allows users to save lead details such as first and last name, designation, lead source, phone number, email, and other key information. Business details can also be added at the time of lead creation, with integration to Companies House enabling automatic fetching of business information into the system. For Website queries submitted from the practice website, contact details such as name, phone and email are mandatory. While only the first name is mandatory while creating manual leads within the system, it provides flexibility to create a lead with minimal details and update additional information over time. A dedicated lead dashboard further supports efficient lead management.	Confirmed

7.06	How does a user track the status of leads?	Software has default lead statuses: Lead, Opportunity, Customer, Lead Lost, Not a Lead and Customer Lost. Users can keep a followup date to track the conversion as well as as well as followups. AO provides flexibility to practices to create multiple stages for better insights. After setting up stages in the practice profile, simply open a lead and assign it to the relevant stage. Leads can also be filtered based on these progression stages, allowing effective monitoring and management.	Confirmed
7.07	Can a user merge multiple individual leads? (e.g. if they are from the same business or duplicated)	Users have flexibility to merge multiple leads into one and link multiple lead contacts to a common business. System automatically detects the phone number and email addresses if already saved in another contact and provide suggestions to directly merge into or link with existing business.	Noted
7.08	Can leads be deleted/archived/reactivated?	Having a cloud based architecture we offer flexibility to manage status and maintian historical data for all the leads. The status of a lead can be updated, however, we do not offer options to delete any communication with a lead or contact from our database. This can be managed only via raising a ticket. Status handling can be done for inactive contacts or a lead that could not be converted into a customer due to unforeseen circumstances can be marked as Lead Lost. Contacts received through calls, chats, or emails that are irrelevant, uninterested, or potential scams can be marked as Not a Lead. If required, you can also reactivate a lead at any time by updating its status to either Lead or Customer.	Noted
7.09	How does a user search for a specific lead? What fields can be used for search?	Acting Office assigns unique lead reference numbers to a concerned lead. In addition to this there is also an Alias option available which can be prompted to provide with a short or a concised name for a lead. Search can be performed based on the following: 1. Lead reference 2. Aliases 3. Phone 4. First name and/or last name 5. Email address	Noted
7.10	Can a user set up notifications for follow ups on leads? If so, how is this set up?	Acting Office ensures that follow-up actions for leads are not missed by integrating follow-up date & time directly into the lead management workflow. When a follow-up date is set for a lead, the system automatically reflects this on the user's dashboard on the mentioned date. Leads are highlighted based on their upcoming follow-ups, prompting timely action. Further, an alert can be set using Internal Callback request for the same lead, which user can either do it for himself or for any other user (e.g. sales team members)	Noted
7.11	How is history of correspondence with a lead or business tracked?	All interactions and updates made against a lead or linked business are captured in the system. Notes, changes in status, updates to contact details, and follow-up actions are recorded in the lead history tab. This provides a complete timeline of correspondence and activities, ensuring that users have full visibility into past communications and decisions whenever they revisit the lead or business profile.	Confirmed
7.12	Can leads be assigned to a user?	Yes. Leads created in Acting Office can be assigned to specific users for better accountability and streamlined management. Assignment ensures that each lead has a responsible user tracking progress, handling correspondence, and following up as required. Once assigned, the lead will also appear on the respective user's dashboard, allowing them to manage their pipeline effectively.	Confirmed
Account (client) creation and management			
7.13	How is a new client added to the solution? What information can be captured for a client?	The status of lead can be changed manually or automatically changes to Customer as soon as acceptance is received on LOE or first payment is made by the client. Businesses will be added to a contact (lead/customer) and will then appears in the businesses list of clients, assigned with a unique Client ID. The solution allows capture of comprehensive details, including: - Basic details such as incorporation date - trading start date, - SIC code, - Trading and registered office addresses, - phone number, - email. - Tax details including the following: >Credentials for HMRC >Agent authorisation 64/8 HMRC, - Subscription details if the client subscribes to services, services availed - Preferences, Notes, Stories, and client reviews for additional references.	Confirmed
7.14	How does a user group or categorise clients? Can the grouping/categorisation be used for search or report?	1. Clients can be grouped and categorised through tags that can be added to a client profile for flexible categorisation. 2. Business type which is displayed in the client list, providing classification at a glance. 3. Filters in the client list, allowing users to apply criteria and sort data as needed. These groupings and filters are directly available for search and can also be leveraged in client reporting, enabling efficient segmentation and analysis.	Noted

7.15	Are there any external information feeds to populate publicly known information e.g. year end dates, addresses etc.	Yes. The system is integrated with Companies House. Each client profile includes a direct hyperlink to the official Companies House record. This ensures users can quickly access publicly available details such as incorporation data, year-end dates, and registered addresses. In addition, important Companies House deadlines are displayed prominently in the client's profile, helping practices manage compliance obligations effectively.	Noted
7.16	What contact information can be attached to a client?	The client profile stores full contact information including: - Email addresses, - phone numbers (with a direct-call option from the profile), - Postal addresses (registered and trading), - Default contact for correspondence. - These details can also be extended to linked client users, who may be provided with portal access through their email.	Confirmed
7.17	How are leads attached to clients?	Leads are created as a contact, and further businesses can be attached to those by changing their status or connecting an existing business using 'Link with business' option, ensuring contacts and associated information are connected appropriately within the client's record.	Confirmed
Quote creation and management			
7.18	What is the process to create a quote?	A quote can be created: 1. from a lead's new business, 2. For an existing business, or 3. Directly through the Quotes section under Sales. With an end-to end flow while setting up new businesses, you can simultaneously utilise the *Save & Quote* option which allows a quote to be generated at the time of business creation. For existing businesses, quotes can be created using the quote icon in the client profile or the shortcut *Shift + Q*.	Noted
7.19	What information is captured in a quote? Can the information be prefilled?	A quote records 1. The creation date (default to today's date), 2. First response contact, 3. Selected services with descriptions and pricing, VAT rates, and optional discounts or notes. Service details and pricing are prefilled from the practice settings and are customisable before saving a quote. Additional services can also be added or removed.	Confirmed
7.20	How does a user send the quote to the client?	Quotes can be sent directly to clients using the *Save & Email* option during creation or through quick action buttons once the quote is saved.	Confirmed
7.21	Is there an approval process for quote creation or communication?	Yes. Clients approve quotes by clicking *Accept* in the email link and this may be typed, drawn, or uploaded. The system records the signatory's details along with the date and time of approval. There is an internal approval process for quotes and engagement letters as well and is something that can be activated and deactivated depending on client requirements.	Noted
7.22	How does the client review and either accept or decline the quote?	Clients receive a secure email link to view the quote. Clients approve quotes by clicking Accept in the email link and this may be typed, drawn, or uploaded. Notifications are sent to the accountant when the client views or responds to the quote. The clients currently don't have the option to decline the quote within the system, instead they can let us know in the email and the accountant can decline it from there end. However, like mentioned at various instances, the option to decline the quote can also be provided, if required.	Noted. Clients can view and accept quotes via a system-generated link. Currently, there is no option to decline the quote within the page itself; any decline must be communicated via email or other external methods. However, the Acting Office offers high customisability and can accommodate this requirement through development if requested by the client. See conclusion point 2.07.
7.23	How does a user track the quote status? Is there any notification for quote status update?	Quotes move through four stages: *Drafted, Sent, Accepted,* or *Rejected*. Users receive notifications when a client views, accepts, or rejects a quote, allowing real-time tracking and follow-up.	Noted
Client Onboarding/KYC			
7.24	How is client identity information captured in the solution?	Client identity information is obtained through data links, where clients can securely upload identity and address proofs. These documents are automatically integrated into the client profile. Additional details such as incorporation data, trading start date, SIC code, addresses, phone numbers, and email are captured directly in the client profile.	Confirmed
7.25	How is AML compliance information captured from the client in the solution?	AML compliance details are managed via the AML tab in the client profile. Officer details are automatically retrieved from Companies House records, and clients can upload identity documents through data links. Accountants can add members manually if needed, and all KYC submissions are stored within the AML section. Completion of the AML Compliance form records declarations, suspicions flagged, and confirmation of adherence to internal risk procedures.	Confirmed
7.26	Can a user customise the information request fields from the client?	Yes. While standard KYC and compliance documents are requested through data links, users can create custom data requests for specific information. These requests can be tailored to each client's requirements and saved in the client profile once approved.	Noted
7.27	Does the solution have tools to perform AML checks?	Yes. Acting Office includes built-in AML verification tools. Users can trigger identity checks for each officer or member, upload or import documents, and generate comprehensive AML reports. Reports provide ratings and risk levels (Low, Medium, High), and a risk dropdown allows users to update severity classifications. Suspicious activity can be flagged and documented as part of compliance.	Noted. See 7.59 for AML tool integration

7.28	How does a user set up client login for the client portal?	From the client profile, the 'Client User' quick action button enables portal access. Users can select a contact email from the dropdown list of saved business contacts. Once saved, the system sends an invitation link to the client, allowing them to create their login and access the portal.	Confirmed
7.29	What information can the client view from their end? And what action can be taken in the client portal?	Clients can: Upload identity and KYC documents and any other requested information through secure data links. Review and accept engagement letters via preset, drawn, or uploaded e-signatures. View and accept quotes, with e-signature capability. Respond to data requests initiated by the accountant. Access their information in line with permissions set in privacy controls.	Noted
7.30	Does the tool have the functionality to create engagement letters?	Yes. Acting Office allows users to create and manage Letters of Engagement (LOEs) directly within the platform.	Confirmed. See 7.31,7.32 for more LOE details.
7.31	Can engagement letters be customised per client or service line, and are there templates for different engagement types (e.g. annual, one-off)?	Yes. Engagement letters are drafted based on the services selected from the practice profile. Each service has pre-defined templates (e.g. CIS, VAT, PAYE, SA100) that auto-populate relevant fields. Users can further edit content for a particular client or service line, enabling both standardised and tailored engagement letters.	Noted
7.32	Does the tool pre-populate key client information into the engagement letter?	Yes. Client information such as business name, contract period, contact details, account manager, and selected services is automatically pre-populated into the LOE. Service-specific data (e.g. number of subcontractors for CIS, payroll frequency for PAYE) is also pulled in from client records.	Noted
7.33	Is there a built-in approval workflow (e.g. maker-checker) before an engagement letter can be sent to a client?	The standard workflow includes draft, send, and accept stages. Engagement letters can be reviewed and edited by the assigned users before sending which can be routed via a well built review mchanism procedure.	Noted
7.34	How are engagement letters shared with clients?	Engagement letters are shared via email directly from the platform. Clients receive a secure link to review the document online and can accept it electronically using multiple signature options. Once accepted, the engagement letter is saved in the system, and the associated services are automatically activated in the client profile.	Confirmed
Invoice & receipt			
7.35	Does the tool have the functionality to generate invoices?	Yes, user can raise invoices in the software. Raising credit notes, creating receipts, managing refunds can be effeciently done in the billing area of our software. Additionally, user can also view and download the invoices from the software itself.	Noted
7.36	How does a user create an invoice?	A user can create an invoice in the system by selecting the currency icon within the software. Additionally, the system also supports automated invoice generation. For example, when a quote is accepted or when a task triggers an action that requires invoicing, the software intelligently generates the invoice automatically, ensuring accuracy and efficiency.	Noted
7.37	What information can be amended when preparing an invoice? Does the tool pre-populate key client and quote information?	The software pre-populates key information when preparing an invoice. Client details, dates, due dates, and quote information (in cases where the invoice is raised from an accepted quote) are automatically filled in for convenience. However, users retain full flexibility to amend these details as needed. In addition, invoices can be edited after creation, and there is also a transfer functionality that allows an invoice to be reassigned to another client if required.	Noted
7.38	For time based services, can time be tracked in the tool to input into invoices?	Our system does not support raising invoices directly based on allocated time. Instead, the quantity for each line item must be specified when creating an invoice. However, we provide a manual timesheet option that allows users to input the number of hours worked for a specific module along with the applicable hourly rate. Based on this information, the system automatically generates an invoice, ensuring flexibility in billing for time-based services.	Noted - timesheet details as per tab "11. Other"
7.39	How is an invoice sent to the client? Can the invoice be sent to the client with set schedule / on a regular basis automatically?	Users have multiple options for sharing invoices with clients. Invoices can be sent directly via email from the system or downloaded for physical dispatch, offering flexibility in communication. Additionally, the system supports recurring invoicing, by setting a desired frequency, invoices are automatically generated at the scheduled intervals, streamlining regular billing processes.	Confirmed
7.40	How does the client review the invoice?	Clients receive the invoice via email, where all key details such as descriptions, amounts, discounts, and VAT are clearly presented. After reviewing the information, they can proceed with payment by clicking the integrated "Pay" button, which redirects them to the secure payment gateway.	Confirmed
7.41	How does the solution manage invoice payment? What are the payment options? (e.g. direct debit, bank transfer etc)	The solution supports multiple payment options through a combination of integrations and manual entry. For online payments, we integrate with Stripe, enabling seamless management of receipts, and with GoCardless, which facilitates a reliable and efficient direct debit mechanism. For clients preferring bank transfers, payments can be recorded in the system through manual entry, ensuring all transactions are properly tracked. This flexibility allows users to manage invoice payments conveniently and in line with their clients' preferences.	Confirmed
7.42	How is the invoice status tracked? Can the solution send notification when the invoice status changes or when an invoice is due?	Managing invoice statuses in Acting Office is both effective and efficient. The system automatically assigns and updates statuses such as Active, In-Progress, Paid, Due, and Deleted without requiring manual intervention. Invoices are seamlessly filtered based on these statuses, providing clear visibility and organisation. Additionally, the system can automatically send reminders to clients when an invoice becomes overdue, ensuring timely follow-ups and improved payment collection.	Noted

7.43	How does the solution manage payment receipts? And how are the receipts sent to the clients?	Acting Office automates receipt management through integrations with Stripe (for card payments) and GoCardless (for direct debits). Payments made through these channels are automatically recorded in the system. For bank transfers, users can manually record full or partial receipts directly from the invoice menu. The solution also supports advance receipts, which can later be allocated against invoices. Clients receive instant confirmation of payments, with a downloadable receipt available from their portal once the transaction is completed. Each receipt is assigned a unique reference number for tracking, and users can also download or email client statements summarising receipts and outstanding balances.	Confirmed
7.44	How does a user manage credit or refund in the solution?	Credit notes for unpaid invoices can be created through the three-dot menu on the invoice. Users specify the date, amount, and reason, and may add remarks for further context. Refunds can be initiated directly from the credit note by selecting the 'Initiate Refund' option. The system allows adjustment of the credit note against outstanding invoices or processing refunds against past receipts. Each refund is logged with a unique reference number, and all refunds are displayed under the Refunds tab, with filters and options for tracking.	Noted
7.45	Which user types in the solution have access to invoice function?	The invoice function is available to all the users. These roles can create, edit, send, transfer, and manage invoices. However, credit notes, receipts, and refunds can also be raised and managed by admin and manger roles only for enhanced security. Access rights can be configured in the practice profile to ensure appropriate segregation of duties.	Noted
7.46	Can the system restrict invoicing or service delivery if an engagement letter has not been signed by the client?	Yes. Acting Office only allows the creation of invoices once a letter of engagement is signed and the quote has been accepted.	Noted
Client Communication			
7.47	What are the communication options available in the solution for the user to contact leads or clients?	Leads can be effectively communicated with through emails or calls. All communication details are securely stored in the system, allowing you to conveniently send follow-up emails or place direct calls to the concerned lead.	Confirmed
7.48	How does a user record notes or complaints from leads or clients?	Users can record notes or complaints directly in the system by raising concerns through the complaints section. This allows management to track, monitor, and resolve issues efficiently while maintaining a clear record of client interactions.	Noted
7.49	How does a user request documents from a client?	Users can request documents from clients through the data request feature in Acting Office. They can initiate requests for details, bank statements, or employee information, ensuring a seamless and efficient exchange of information.	Confirmed
7.50	What templates are available for client communication? (e.g. Letters, information requests, quotes, services etc) Can a user modify the templates?	Templates in Acting Office can be added and fully customised to meet user requirements. Using the tags functionality, users can insert dynamic placeholders within the content, which automatically update with client-specific information stored in the system, ensuring personalised and efficient communication.	Noted. Available templates as per each functionality section answers, available for LoE, quotes and information requests etc.
7.51	What security features are used for document or information sharing (e.g. OTP, authentication code, e-signatures)?	Documents can be shared with clients in a highly secure and controlled manner through our one-time password (OTP) mechanism. When a document is shared, the client automatically receives a unique OTP delivered to their registered email address. To access the document, the client must enter this OTP in the designated verification field, ensuring that only the intended recipient can view the content. This additional layer of security not only safeguards sensitive information but also reinforces trust and confidentiality in all client communications.	Noted. OTPs to mobile/SMS as a MFA method, are not the most secure method of MFA as they are able to be compromised, and there have been a number of cyber incidents recently arising from the use of SMS based MFA. As such, MFA via authenticator app is strongly preferred. See conclusion point 2.03
Reporting/ Analytics			
7.52	Are there dashboards available in the solution, and if so, which ones are provided? (e.g. client, quotes, revenue, pipeline etc)?	Acting Office features an intuitive dashboard for easy access to key information. A dedicated dashboard is also available for Admin users, providing deeper insights into financial performance and lead management. In addition, specialised dashboards are available to track timelines, revenue, and collections for more effective management.	Noted
7.53	Can users customise existing dashboards and/or create new ones?	Currently, dashboards in Acting Office are pre-designed to provide key insights and cannot be customised or newly created by users. However, they are structured to cover the most relevant aspects of practice, financial, and lead management to ensure comprehensive visibility. You do have required status and date filters with you to cutomise the dashboard as per your requirement.	Noted
7.54	What actions can a user take from within the dashboards (e.g., modify records or information)	The intuitive dashboard enables users to efficiently manage their activities in one place. From adding tasks and managing leads to addressing urgent actions and tracking follow-ups, all key functions can be performed directly within the dashboard.	Confirmed
Configuration / Administration			
7.55	Are there differences between the mobile app and website functionality for the CRM module?	Mobile app is still under development and currently it only supports Calls and Chats functionality. However, you can use the Acting Office platform from the mobile using the internet browser.	Noted. Currently the mobile app's CRM feature is limited to calls and chats. There is activity on the roadmap to expand this functionality. See conclusion point 2.06.
7.56	How does a user set up notifications or alerts in the solution?	Acting Office ensures that all important communications are delivered to the respective users through automated email alerts. Practices can benefit from these carefully designed notifications and also customise which alerts should be shared, based on their needs and preferences. The client provides us with a list of notifications and reminders that they need and then the IT team sets those up in the background based on the requirements.	Noted. Standardised notifications are available for configuration by the administrator within the application. For any notification requirements beyond the standard configuration, clients may raise a support ticket, and the Acting Office will assist with the custom setup. See conclusion point 2.07.

7.57	How are documents managed in the solution? Are there any controls around who can access these documents?	The Document section in Acting Office is designed as a centralised storage hub for all important files, ensuring quick and convenient access. Any information or documents shared by customers are automatically saved here, and users also have the flexibility to create or upload documents manually as needed.	See 11.14 for access control.
7.58	What customisation is allowed in the CRM module?	The CRM module provides extensive customisation options to meet your practice needs. You can define custom lead stages, create tailored fields to capture specific client information, configure user roles and permissions, and personalise dashboards for improved visibility. Integrations with third-party applications can also be enabled to streamline processes and enhance functionality. Additionally, a customisable icon allows you to adjust report columns as per your specific requirements.	Noted
7.59	Does the solution integrate to any third party tools? If so, please provide integration examples (e.g. communication, payment, AML etc.).	The system also integrates with third-party applications to enhance functionality. Key integrations include Veriphy for AML checks, Twilio for communications, and Stripe and GoCardless for payment processing.	Noted

Ref	Requirement	Response	Reviewer Comments
8.	**Payroll**		
System overview			
8.01	What is the high level process flow for the payroll module and what are the key user access roles?	The payroll process in Acting Office follows a structured flow: employee setup → pay run scheduling → payroll processing → FPS/EPS submission to HMRC → payslip and report generation. The roles are the same within the entire Acting Office system categorised into Admin, Manager and Staff user roles. Each level user role can be customised on request, for example, manager can submit the PAYE but not a staff user. The team leader role falls within the Admin or Manager level access. The team leader role is simply a categorisation aimed at providing some specific set of reporting capabilities like viewing the team members, tasks, their calenders etc in order to ensure work management.	Noted.
Payroll Setup and Admin			
8.02	How does a user set up payroll function for a client? What is covered in the payroll settings?	The payroll function for a client can be setup by adding important information such as the tax year, PAYE reference, HMRC office number, and other important details in the setting up wizard. All the information saved during the setup proces can be later on edited from the settings tab. Additionally, settings tab also provide accessibility to save details to run auto payrolls, configure notifications, connect pension software providers such as Nest and SmartPension and add employee logins for a concerned client.	Noted
8.03	What are the key data fields needed to configure a payroll run?	Essential fields include employee personal details, tax code, NI details, gross or net pay, payment frequency, director status, pension scheme, student loan or postgraduate loan status, and deductions or additions.	Confirmed
8.04	How does a user add payroll information into the solution (e.g. manual, upload file, integration)?	Information can be added manually, via bulk import templates, or through secure client data requests in which the client can directly provide a list of information for their employees using a secure link which can be accessed by the respective accountants. Integration with Companies House and secure links further streamline updates.	Confirmed
8.05	How is payroll date and frequency managed in the solution? Can the payroll frequency be set up differently for different employees?	Payroll frequencies such as weekly, monthly, or annually can be set per client or adjusted per employee using the *Change Pay Frequency* utility, providing flexibility.	Confirmed
8.06	Does the solution support the use of different cost centres for different employees?	Yes, the employees can be categorised into different departments. The departments can be created and then employees can be categorised in different departments accordingly.	Noted
Pay Calculation and Deductions			
8.07	How are bonuses or commission managed in the solution (e.g. how is variable pay added to a regular payroll)?	Bonuses, commission, and variable pay are recorded under *Additions and Deductions*, ensuring accurate inclusion in gross pay and compliance with HMRC reporting.	Confirmed
8.08	How are changes in salaries / benefits communicated to HMRC and subsequent tax codes changes received?	Updates to salaries or benefits are processed in the system, reflected in FPS submissions, and HMRC notifications (such as new tax codes) are automatically retrieved in the notification tab.	Confirmed
8.09	How is retroactive pay / backdated pay adjustment applied to the current payroll in the system?	The system allows you to process the payroll for the previous periods without a late submission reason dropdown. Further, if the current period payroll has already been processed, then in order to process a backdated payroll, you can undo the payroll and then do the previous submission and then an amended submission for the period already submitted. By doing the above, the HMRC gets the updated YTD figures.	Noted
8.10	How is shift-based pay managed in the solution (e.g. night or weekend premium, overtime etc.)?	Shift allowances, overtime, and premiums (e.g., night or weekend rates) are managed as additions under the employee's payroll profile and included in pay calculations.	Noted
8.11	How is leave or absence recorded in the payroll for pay adjustment calculation?	Leave and absence are recorded in the employee profile under leave management, with start and end dates. Relevant statutory leave types are supported such as maternity, paternity, adoption, shared parental, annual leave.	Noted
8.12	How is holiday pay managed in the solution?	Holiday pay is calculated based on pay frequency and employee details, with entitlement tracked in the leave section. Carry-over rules can be configured in settings section.	Noted
8.13	How is the final termination pay calculated in the solution (e.g. unused leave, last working day and other settlements)?	The final termination pay needs to be calculated manually and then the figures need to be accordingly inputted into the system.	Noted
8.14	What is the approval flow for payroll generation and payment? How is this shared with the client?	Payroll runs can be shared with clients via email confirmations prior to FPS submission. Clients may review through secure links, after which the payroll is finalised and submitted.	Confirmed
8.15	Does the solution manage expense payments for employees? If so, how are expenses managed in the solution?	Yes. Expenses are entered and managed under *Expenses and Benefits*. They are reported to HMRC where applicable and included in payroll calculations.	Confirmed
8.16	How are pension contributions captured and calculated in the payroll?	Pension schemes are created in Acting Office with contribution type, tax relief, and earnings basis configured. Employees are assigned schemes and contributions are auto-calculated in each pay run.	Confirmed
8.17	How are salary sacrifice schemes managed in the solution?	Salary sacrifice is supported through deductions in payroll and pension scheme configurations, ensuring correct tax and NI treatment.	Confirmed
8.18	How are additional taxable benefits managed?	Taxable benefits are recorded under *Expenses and Benefits* and are included in P11D submissions for HMRC compliance.	Noted
8.19	How are student and postgraduate loans managed in the solution?	Loan status and plan type are recorded in employee details. Deductions are automatically calculated in payroll and reported via FPS.	Confirmed
8.20	How is director payroll and NI managed in the solution? (for alternative calculations or net-to-gross calculation)	Directors can be flagged in employee setup. Acting Office supports annual or alternative NI calculation methods, with correct application in pay runs.	Confirmed
8.21	Is there an option to set up charity donation from the payroll payment? If so, how is payroll giving managed?	No, no option as of now.	Noted
Payment			
8.22	How are net salary payments managed in the solution? Can payment runs be managed from the solution?	Net pay is calculated within pay runs, and payment runs can be managed in Acting Office, including scheduling and exporting payment instructions.	Confirmed
8.23	Is the solution integrated to any pension providers? How are both employee and employer contributions to pension providers managed?	Yes. Pension contributions for both employee and employer are recorded in pay runs and can be exported or integrated with pension providers. We have our integrations with renowned pension providers such as Nest and SmartPension, which facilitates seamless transfer of information with respect to pension.	Confirmed.
8.24	How are tax and NI payments to HMRC tracked and managed? Can payment runs be managed from the solution?	Tax and NI liabilities are calculated in each run, reported via FPS/EPS, and tracked through HMRC payslip reports. Payment runs can be generated for HMRC remittance in our software.	Confirmed
Compliance and Taxation			

8.25	How are FPS, EPS and other HRMC reports managed?	Acting Office automates FPS and EPS submissions within payroll runs. Other HMRC reports (NVR, CIS, etc.) are supported through dedicated utilities.	Confirmed
8.26	How are end-of-year fillings (P60s, P11Ds and other relevant forms) managed in the solution?	End of year documents like P60's are generated automatically as soon as the final payroll of that particular year is submitted to the HMRC. In regards to P11D's, those can be created and submitted to the HMRC from the Acting Office system itself.	Noted
8.27	What validations exist before submission (e.g. minimum wage).	System checks ensure compliance with minimum wage, pension eligibility, employment allowance, and other statutory requirements before FPS submission.	Noted
8.28	How is P32 managed in the solution?	The system generates a P32 report, which summarises an employer's monthly or quarterly Tax and National Insurance (NI) liabilities to HMRC. Users can also produce the report for custom periods, with the option to download it in a convenient format. Also, with the automations in place, the system can also automatically send the P32 reports to the employer.	Noted
8.29	How is HMRC RTI (real time information) managed in the solution? How are HMRC RTI Errors received and managed?	RTI submissions are handled within payroll runs. HMRC responses and error notifications are automatically retrieved in the notification tab in the settings section for corrective action.	Noted
8.30	Can the solution generate P45 forms for existing employees?	Yes. P45s are automatically created upon employee termination, including tax and pay details to date.	Noted
8.31	Does the solution support the incorporation of P45s for new employees (from their previous employer)?	Yes. Employee setup allows entry of P45 details to ensure correct tax code and YTD figures are carried forward.	Noted
8.32	How is CIS return report managed in the solution?	The CIS module supports subcontractor management, CIS300 return preparation, and YTD reporting for HMRC.	Noted
8.33	How are statutory payments managed (e.g. Statutory Maternity Pay, Statutory Paternity Pay, Statutory Adoption Pay etc.)?	Statutory payments are managed within leave management. Acting Office calculates entitlements and reflects them in payroll and EPS submissions.	Noted
Employee Service			
8.34	Is there an employee portal in this solution for employee self service?	Yes, the employee portal is available for employee self-service.	Confirmed
8.35	If yes, what information can employees view from the employee portal? (e.g. payslips, P60s)	Employees can view personal information, employment details, Payslips, P45, P60, Payroll Summary and leave entitlement details.	Noted
8.36	If yes, can employees update their personal information in the employee portal? If so, what information fields can be updated?	Not at the moment, but this is something that we will introduce in our next phase.	Noted. Employees cannot update information in the employee portal currently. There is activity on the roadmap to expand this functionality. See conclusion point 2.06.
8.37	Can employee payslips be bulk downloaded/shared?	Yes. Payslips can be bulk downloaded in PDF or Excel format and shared directly by email.	Noted
Reporting/Analytics			
8.38	Does the solution provide payroll summary reports? Are there any other payroll related reports available? (payroll forecast, YTD etc?)	Yes. Reports include payroll summaries. Acting Office provides multiple reports for user's convenience for better analysis in the form of YTD reports, P60, P45, payslips, HMRC payslip, expenses, benefits, and forecasts for PAYE, NI, and deductions.	Noted
8.39	Can the user customise reports in the payroll module?	Yes. Reports can be filtered by employee, pay frequency, or period, and exported in detailed or summarised formats which can also get downloaded in the PDF/Excel versions as well.	Noted
8.40	How are such reports communicated to the client? Would the client have direct access to the payroll module specific to its company?	Reports can be exported and emailed directly. User can also download the required document and can share the concerned file physically. At the moment, Acting Office does not provide the feature to allow direct access to the payroll module for the specific company. However, all the information can be shared to the respective accounatnt via the secure link to maintain a smooth transmission of information from the client.	Noted
Configuration / Administration			
8.41	Does the solution integrate to any third party tools? If so, please provide integration examples.	Yes. Acting Office is integrated pension providers such as Nest and SmartPension for contribution uploads, and HMRC systems for RTI submissions and notifications.	Noted
8.42	What customisation is possible in the payroll module?	Customisation includes pay frequencies, departments, holiday calendars, payslip formats, pension schemes, contribution types, and reporting layouts.	Noted
8.43	How does the payroll information post to Bookkeeping or Accounts & Tax module?	Payroll journals are automatically generated upon FPS submission and posted to the bookkeeping module, ensuring synchronisation with accounting records.	Noted

Ref	Requirement	Response	Reviewer Comments
9.	**Bookkeeping**		
System overview			
9.01	What is the high level process flow for the bookkeeping module and what are the key user access roles?	The bookkeeping module follows a structured process: setup of client business → recording sales, purchases, expenses, dividends, assets, and journals → managing bank transactions and reconciliations → VAT return preparation and submission → reporting and analysis. There are no user roles assigned to this module. However, in addition to this client can also perform their bookkeeping on their own using designated credentials. Each level user role can be customised on request, for example, manager can submit the VAT return but not a staff user.	Noted. By default, no user roles are assigned to the bookkeeping module. However, if role-based access control (RBAC) is required, clients can raise a support ticket, and the Acting Office will assist with the necessary customisation.

See conclusion point 2.07. |
Accounts Payable / Purchases			
9.02	How is supplier information managed in the solution? What information is captured?	The bookkeeping module in Acting Office provides a dedicated suppliers section where users can add and manage supplier records. New suppliers can also be created directly at the time of raising an invoice. Integration with Companies House enables automatic syncing of available business information, which can be further edited as required. The system captures comprehensive supplier details, including name, contact information, VAT and EORI numbers, bank details, payment terms, and notes.	Noted
9.03	How does a user create a purchase order in the solution?	Purchase orders are generated similar to invoices by selecting suppliers, items, quantities, prices, and VAT rates. Once saved, the PO can be converted into an invoice seamlessly in Acting Office.	Noted
9.04	Does the solution record the list of items/ service from suppliers for purchasing?	Yes. Items (products/services) are stored with codes, descriptions, VAT rates, purchase/sales prices, and can be reused across invoices and orders.	Noted
9.05	Does the solution support the generation of a goods receipt note?	Yes. Goods receipt details can be recorded and linked to purchase orders and invoices.	Noted
9.06	How are supplier invoices received and logged in the tool?	Invoices can be created manually, imported via CSV, or generated from scanned/uploaded documents (OCR). Supplier details and references are automatically populated.	Noted
9.07	How are supplier payments approved?	Payments are initiated through the Add Payment function, with workflows allowing review and approval before final posting.	Noted
9.08	Does the system perform any validation controls (e.g. three way match) before approving payment?	Yes. The system supports three-way matching (PO, goods receipt, invoice) and flags mismatches for review.	Confirmed
9.09	How does a user record the payments to suppliers in the solution?	Payments are recorded manually or imported, with auto-allocation across outstanding invoices using FIFO. Excess payments are stored as supplier advances.	Confirmed
9.10	Does the solution manage supplier credit notes and/or refunds? If so, what information is captured?	Yes. Credit notes can be created against invoices with details of items, quantities, VAT, and refunds. They can be applied to outstanding invoices or recorded as supplier refunds.	Noted
Accounts Receivable / Sales			
9.11	How is customer information managed in the solution? What information is captured?	The bookkeeping module in Acting Office provides a dedicated customers section where users can add and manage customer records. New customers can also be created directly at the time of raising an invoice. Integration with Companies House enables automatic syncing of available business information, which can be further edited as required. Captured information includes contact details, VAT/EORI numbers, payment terms, credit limits, discounts, and notes.	Confirmed
9.12	How are purchase orders received from customers captured in the solution?	Customer PO cannot be created within the system but those received from customers can be attached against sales invoices, ensuring traceability.	Noted
9.13	How are customer goods receipt notes captured in the solution?	Customer good receipt notes can be recorded and linked to invoices for reconciliation.	Confirmed
9.14	How are sales invoices managed in the solution?	Sales invoices can be created manually, auto-populated from estimates, or imported. The system supports VAT handling, discounts, attachments, and emailing directly to customers.	Noted
9.15	How are received customer payments tagged to the relevant invoice?	Receipts are recorded manually, via import, or through bank feeds. Auto-allocation links payments to outstanding invoices on a FIFO basis, with manual allocation also available.	Noted
9.16	Does the solution manage customer credit notes and/or refunds? If so, what information is captured?	Yes. Credit notes can be created against invoices with full details, and refunds can be processed to customers where applicable.	Noted
Expenses			
9.17	Does the tool have expense management functionality?	Yes. Acting Office supports expense claims, reimbursements, and refunds for efficient and effective expense management.	Noted
9.18	If so, how are expense claims recorded in the solution? Will this be recorded automatically if the client is using both payroll and bookkeeping module?	Claims are created manually by adding users and line items. If both payroll and bookkeeping modules are used, approved expenses can flow into payroll for automatic processing.	Noted - see tab "8. Payroll" for more details for expense management
9.19	How are expense types, cost centres, receipts recorded against expense claims in the solution?	Each claim records account codes, VAT, cost centres, amounts, and receipts/attachments.	Noted
9.20	Are there approval processes for the expense claims in the solution? If so, how are they managed?	Yes. Expense claims can be reviewed, approved, or rejected with audit trails maintained.	Noted
9.21	How are reimbursement payments recorded in the solution?	Reimbursements are entered with allocation against expense claims, and payments posted to the relevant bank accounts.	Noted
9.22	How is expense owner information managed in the solution? Can the user allocate cost centres and claim limits to the expense owners?	Expense owners are linked to claims, with options to assign cost centres and set claim limits.	Noted
Dividends			
9.23	How does a user add shareholders in the solution? What information is recorded for a shareholder in the solution? Can the solution import the shareholder information from Companies House?	Shareholders can be imported from Companies House or added manually with details including name, contact information, share type, and number of shares.	Noted
9.24	How are dividends managed in the solution? What information does the solution capture for dividends?	Dividends are created as vouchers, capturing shareholder details, dividend per share, and total amounts.	Noted
9.25	How are the dividend types, number of shares, class recorded in the solution?	The system records share classes, number of shares, and dividend amounts, with automatic journal posting.	Noted
9.26	Does the solution restrict user to post dividends if there is a loss?	Yes. The system validates available profits before permitting dividend distribution. If an attempt is made to declare dividends in the event of a loss, a warning message is triggered to alert the user.	Noted
Assets			
9.27	How are fixed assets recorded in the solution?	Assets are added with purchase details, supplier/bank, VAT, depreciation method, rate, and useful life.	Noted
9.28	How does the solution support various asset depreciation methods?	Supports straight-line and written-down value methods, with automated depreciation journals and rollback functionality.	Noted

9.29	How does the solution support the disposals of assets?	Disposals record proceeds, calculate profit/loss, and generate corresponding journals. Disposed assets can be reactivated if needed.	Noted
Journals			
9.30	How does a user create a journal in the solution?	Journals can be entered manually with accounts, VAT, debit/credit, and descriptions. In addition to this, system also records automatic journals, from the relevant section or entry.	Confirmed
9.31	Can journals be imported; what input methods are supported (manual, OCR, CSV, bank feeds)?	Currently, journals cannot be imported. However, users can create journals manually, and the system also generates automatic journals for processes such as bank imports, dividend declarations and while while charging depriciation.	Noted
9.32	Are there validations for duplicate or miscategorised entries?	Yes. The system checks for duplicates and validates entries against the chart of accounts.	Confirmed
Banking			
9.33	Does the solution interface directly to third party banks?	Yes. Bank feeds enable direct import of transactions, alongside CSV uploads and manual entry.	Confirmed
9.34	How are transactions imported?	Transactions can be imported from bank feeds, CSV templates, or added manually.	Confirmed
9.35	How are transactions categorised (e.g. AI suggestions, rules)?	Categorisation uses AI suggestions, bank rules, and user-defined rules. Cash coding allows bulk categorisation.	Confirmed
9.36	How does the tool support reconciliation between the accounts and cash in bank?	Reconciliation matches imported transactions with invoices, receipts, and payments, with visual status indicators for explained/unexplained items.	Confirmed
9.37	Is there automatic linking between transactions and customer and supplier invoices?	Yes. Transactions are automatically matched to customer or supplier invoices where references align.	Noted
9.38	Are there validations for duplicate or miscategorised entries?	Yes. Duplicate imports and miscategorised entries are flagged for review.	Confirmed
VAT			
9.39	Does the solution integrate with HMRC's Making Tax Digital (MTD) system?	Yes. Acting Office is fully integrated with HMRC's Making Tax Digital for VAT submissions.	Confirmed
9.40	How does a user enter VAT records? Can the user import records from files or through integration? What information is needed for a user to create VAT records for the first time?	VAT details such as the VAT number, registration date, scheme, frequency are captured at setup. Records can be imported, manually entered, or integrated from transactions.	Noted
9.41	Does the solution auto calculate VAT liabilities and handle multiple VAR rates? If so, how is the auto-calculation managed?	Yes. VAT is calculated automatically across invoices and transactions, supporting multiple VAT rates, that can be setup either in the setup wizard or from the setting section.	Noted. See 10.02 for Setup Wizard details
9.42	How does the user manage VAT return period (quarterly vs annually) or late claims?	Return frequencies are configurable monthly, quarterly, annual. Late claims can be rolled into subsequent returns.	Confirmed
9.43	Does the solution support multiple VAT schemes (e.g. Standard VAT, Flat Rate Scheme, Cash Accounting Scheme, Margin Scheme, and Retail Schemes.)? Please provide details on which VAT schemes this solution supports.	Yes, Acting Office supports the following schemes: 1. Standard, 2. Flat Rate, 3. Cash Accounting	Noted
9.44	Does the solution flag issues like duplicate entries, missing invoices, or incorrect tax codes in VAT return? If so, please provide details on what issues the solution can flag for VAT return.	Yes. Any duplicates, missing invoices, and incorrect tax codes before return submission are flagged in Acting Office for user convenience.	Confirmed
9.45	How does a user submit the VAT return to HMRC from the solution?	VAT returns are filed directly via MTD integration, with acknowledgment receipts stored.	Confirmed
9.46	How does the solution manage the internal review and approval, external client review and approval processes for VAT return?	Returns undergo preparer review, reviewer approval, and client approval before submission.	Confirmed
Reporting			
9.47	What dashboards are available in the solution?	Dashboards provide overviews of cashflow, P&L, balance sheet, invoices, purchases, expenses, and tax timelines.	Confirmed
9.48	Can a user customise the reports?	Yes. Users can customise layouts, filters, decimal displays, and add commentary. All these can be configured in the settings sections of the Bookkeeping module.	Confirmed
9.49	What actions can a user take from the dashboards? (e.g. modify the records/ information)	Dashboards allow drill-down to underlying records, creation of entries (invoices, receipts), and quick report generation.	Confirmed
9.50	How does a user generate financial statements? (Balance sheet, P&L, Cash flow)	Balance Sheet, P&L, and Cashflow reports are auto-generated from trial balances and journals.	Confirmed
9.51	How is budget vs actual reported?	Budget Manager in Acting office enables creation, import, and comparison of budgets with actuals, supported by variance reports.	Noted
Configuration / Integration			
9.52	How does a user set up business details for a client? What information is captured for a book?	Business setup includes SIC codes which is auto-fetched from Companies House, category (product/service), start date, and mode of import for historic records, Vat details and bank records.	Noted
9.53	How are VAT details set up in the solution?	VAT registration details, schemes, and return frequencies are entered during setup, with options to edit later. In addition to this, these can also be configured from the settings section.	Noted
9.54	How are bank details set up in the solution?	Bank accounts are added with type, name, number, sort code, IBAN, and can be marked as primary.	Noted
9.55	How are chart of accounts managed and customised?	The system includes predefined codes, with options to add, edit, or archive user-defined accounts.	Noted
9.56	What customisations are possible in the bookkeeping module?	Users can customise templates, numbering sequences, VAT rates, reports, and dashboard views.	Noted
9.57	How does the Bookkeeping module interface with the other modules?	Bookkeeping integrates with Accounts & Tax, Payroll, and CRM, ensuring consistent data flow across modules within Acting Office.	Noted
9.58	Does the solution integrate to any third party tools?	Yes. Integrates with Companies House, HMRC (VAT), and external bookkeeping tools such as Freeagent for imports.	Noted

Ref	Requirement	Response	Reviewer Comments
10.	**Accounts & Tax**		
System overview			
10.01	What is the high level process flow for the Accounts & Tax module and what are the key user access roles?	The Accounts & Tax module follows a structured process: business setup → trial balance creation/import → accounts preparation → tax computation → internal and client review → submission to HMRC and Companies House. The roles are the same within the entire Acting Office system categorised into Admin, Manager and Staff user roles. Each level user role can be customised on request, for example, manager can submit the accounts and tax but not a staff user. The team leader role falls within the Admin or Manager level access. The team leader role is simply a categorisation aimed at providing some specific set of reporting capabilities like viewing the team members, tasks, their calenders etc in order to ensure work management.	Noted
Accounts			
10.02	How does a user set up business records for a client for the first time? What information is captured?	A setup wizard guides users through three stages: **Business defaults**: business size (small/micro) and trading status (trading/dormant). **Accounting periods**: auto-retrieved from Companies House, with the option to add manually. **Business contacts**: officers auto-fetched from Companies House, with the ability to add officers or create director-specific accounts.	Noted
10.03	How does a user create/add a trial balance in the solution? What integrations exist for trial balance import?	Users can create a trial balance manually or import via CSV, bookkeeping module, or integrations with external software through secure API connections. Accounting periods are auto-fetched from Companies House but can be added manually.	Noted
10.04	How does a user edit trial balances in the solution? Can adjusting journals be added post-import?	Trial balances can be edited using the *Edit* function. Users can either post manual journals or import additional CSV files. Adjusting journals remain clearly distinguishable from the original data.	Confirmed
10.05	How are anomalies in trial balance flagged and resolved?	Comparative trial balance reports highlight period-on-period variances. Unmapped or unmatched codes are flagged during import, with options to link to existing accounts or create new ones.	Confirmed
10.06	Which reports does the solution support in the generation of?	There are various reports in Acting Office to manage the information of the records which include statutory accounts (full, abridged, filleted), management accounts, trial balance comparisons, and corporation tax computations.	Confirmed
10.07	How are these reports templated?	Reports are auto-generated from trial balances using pre-configured templates aligned with Companies House and HMRC requirements. Users may adjust templates to include comparatives, notes, and policy details as well in our software.	Confirmed
10.08	Are these reports interactive? E.g. allow users to click through the report sections for more details? If so, please provide more information on what details users can see from click through the account reports.	Yes. Users can navigate within reports, expand sections, and view linked trial balance details, accounting policies, or attached notes for greater transparency.	Confirmed
10.09	How can these reports be amended / added commentary against?	Users may edit notes, accounting policies, and report sections directly, with options to include additional commentary or disclosures. Changes can be saved to business settings for future use.	Confirmed
10.10	How are these reports submitted to Companies House?	Reports are submitted electronically via the Submit function, with validations performed prior to filing. Credentials are required, and acknowledgments can be polled to confirm submission.	Noted
10.11	Can auditor reports be incorporated into annual reports?	Yes. Auditor or accountant reports can be added via the notes section, with signatories and firm details editable before inclusion in the final report.	Noted
Tax			
10.12	What tax returns does the solution support a user in calculating and submitting (e.g. CT600, SA100 etc.).	The system supports corporation tax (CT600), self-assessment (SA100), partnership (SA800), and related supplementary schedules.	Noted
10.13	What are the high level process steps for completing the various tax returns?	Steps include: importing accounts data → calculating adjustments (disallowables, capital allowances, losses, R&D claims) → preparing tax computation → review and validation → e-signature approval → submission to HMRC.	Noted
10.14	How are changes in tax legislation updated in the system?	Updates are incorporated into the software through regular releases, ensuring computations, forms, and validations remain compliant.	Noted
10.15	How are late claims and adjustments handled?	The system supports amendments through revised returns, with options to mark reports as Amended and automatically tag iXBRL outputs accordingly.	Noted
10.16	Are digital forms available for client data collection?	Yes. Clients can provide data through secure online data links that are sent by their respective accountants, reducing manual data exchange.	Confirmed
10.17	How are journals for the completed tax returns posted to the trial balance?	On completion of CT600, the system auto-posts corporation tax liabilities to the trial balance. Manual updates are also possible.	Noted
Review and Submission			
10.18	How does a user send reports (account, tax etc) for internal and external review in the solution? How does a user set up the review approval chain?	Reports can be sent for internal review via Send Review Request. Users assign reviewers, attach workings, and track responses. The reviewer can be selected from the dropdown and the appropriate reviewer will get notified of the same either via email and an update will be made in the action center of the concerned individual.	Confirmed
10.19	How does a user submit the final reports to the client?	Reports are shared through secure links with e-signature functionality, allowing clients to review, comment, and approve electronically.	Confirmed
10.20	Are submission responses stored and auditable?	Yes. All responses from HMRC/Companies House, as well as client approvals, are logged with timestamps for full auditability.	Noted
10.21	What validations exist before submission to HMRC/Companies House?	The system checks for compliance with statutory requirements, missing disclosures, and calculation inconsistencies. Errors must be resolved before submission; warnings and comments may require commentary.	Noted
10.22	Can submission be blocked until client approval is received?	Yes. Submissions cannot proceed until client e-signature approval is obtained, ensuring proper authorisation.	Noted
10.23	How are reports / completed forms be submitted to HMRC?	Tax returns are submitted electronically using agent or business credentials, with validations and IRMark confirmation provided.	Noted
Reporting			
10.24	What dashboards are available in the solution?	There is no specific dashboard as such for accounts and tax module but it does give you a list of all the clients with there year ends and due dates.	Noted
10.25	Can a user customise the reports?	Yes. Users can configure layouts, add/remove pages, insert notes, and apply business-specific customisation.	Noted
10.26	What actions can a user take from the dashboards? (e.g. modify the records/ information)	From dashboards, users can view report status, modify records, manage queries, and initiate reviews or submissions.	Noted
Configuration / Integration			

10.27	What types of businesses does the tool support (e.g. Ltd, LLP, partnerships, sole traders, trusts, charity etc.)	The Accounts and Tax module currently supports limited companies, LLPs, sole traders and partnerships. Development is currently underway to incorporate registered trusts and charities for this module.	Noted. Trust and Charity entities are not currently supported by the Accounts and Tax module. There is activity on the roadmap to expand this functionality. See conclusion point 2.06.
10.28	How does a user configure account reports template in the solution?	Report templates are managed in the Settings menu, where users can edit notes, pages, and report types for future use.	Noted
10.29	How does the client finance team access the solution? What is the difference between external client and internal user access?	Client's finance team will have visibility of the finance reports within the platform. However, firms have an option to use REST APIs to fetch billing data from AO to their systems. Clients have a separate login which gives them access to their bookkeeping and a range of other options like paying the invoices, accepting quotes, sharing information, viewing documents etc but it does not allow them to get into the solution as a whole.	Noted
10.30	What customisation is allowed in the accounts and tax module?	Customisation includes report layouts, notes, accounting policies, chart of accounts, and page inclusion.	Noted
10.31	How are business rules and automation enabled in the solution?	Automation is embedded through rules such as mapping accounts, auto-populating notes, tax calculations, and system validations. Custom rules can also be configured.	Noted
10.32	How does the Accounts & Tax module interface with the other modules?	Trial balances can be imported from Bookkeeping, payroll journals posted directly, and reports integrated with client dashboards.	Noted
10.33	Does the solution integrate to any third party tools?	Yes. Integrations include Companies House to auto-fetch of officers/periods, HMRC for submissions, and Freeagent to import trial balance.	Noted

Ref	Requirement	Response	Reviewer Comments
11.	**Other**		
Task & Time Tracking			
11.01	How are user tasks tracked in the solution? How are new tasks created in the solution?	Tasks in Acting Office are tracked through structured workflows split into task steps, each with real-time statuses (Waiting, In Progress, Completed, N/A). Updates occur automatically via workflow triggers or can be managed manually. Users track tasks from the dashboard (colour-coded by priority), client profile, or central task list, with a full history log maintained for transparency. Tasks are created either automatically (e.g., via Companies House integration) or manually through the client profile or task section. When creating a task, users define type, client, title, action date, due date, deadline, priority, and assignee, with the option to attach documents and mark tasks as client-specific.	Noted
11.02	How are timesheets managed in the solution? Can users track time manually and automatically in the solution?	Timesheets in Acting Office can be managed per user, with time automatically tracked across calls, emails, modules, and client activities. Users can also view team-wide time statistics. Where needed, time can be logged manually using the manual timesheet option.	Noted
11.03	What report is available for task management?	A dedicated timesheet report provides detailed insights into user and team time statistics, supporting task management and productivity tracking.	Noted
11.04	How is the time tracked for each task?	AO's automated timesheet specifically tracks the user-activity for default KPIs and is linked with workflows to ensure work has been completed with the stipulated timeframe	Noted
11.05	Are there validations to ensure minimum daily hours are logged?	Every practice has it's own benchmark, hence, it is upto the practices to decide the minimum billable hours. Number of working hours can be configured for data validation by the IT team at the time of setting up the client practice.	Noted
11.06	Can time entries be linked to specific clients, tasks, or services?	AO keeps a track of manual and automated timesheet to understand user activity and billed hours. Manual timesheet entries can be manually linked to clients in order to keep track of billable hours.	Noted
11.07	Is there a review or approval workflow for submitted timesheets?	There are 2 separate reports: 1. Timesheets (manual + automated) 2. Workflow reports (detailing the user completed, due, or upcoming workflows), to manage service deliveries for service excellance team. Please note that there is no approval flow for the timesheet submitted in the out-of-box solution. However it can be configured and included in the workflow reports if needed.	Noted. The timesheet functionality does not include an approval workflow by default. However, if approval functionality is required, clients can submit a request to the Acting Office, which can support custom workflow development. See conclusion point 2.07.
11.08	Can time entries be converted into WIP and linked to billing? If so, how is user rate and WIP billing managed in the solution?	With the timesheets, it is progressed via recording it as a WIP and then while creating an invoice, it validates any of the WIPs for the client and then auto-fetch the bill values which are editable for further changes to invoice. The time entries will be converted to WIP at the end of the day with charge rates provided. The WIP can be included in the client invoice. WIP amount can be edited to match invoice amount or reported as loss.	Confirmed
Support & User Guide			
11.09	How does a user submit a support request? Does the solution have live chat support?	Acting Office provides an in-built ticketing system for raising support requests. Users can log requests, report issues, or suggest enhancements directly within the software. Each ticket is automatically assigned to the relevant support team, acknowledged, and tracked until resolution. At present, the solution does not include a live chat feature; however, the ticketing system ensures that all support needs are properly logged and addressed.	Noted
11.10	How does a user for in-app guidance?	In-app guidance is available through help icons located throughout the solution. Clicking these icons redirects the user to a comprehensive help page, which contains detailed documentation, step-by-step guides, screenshots, and instructional videos. This ensures that users have on-demand access to practical resources without leaving the application.	Confirmed
Collaboration			
11.11	Can different users work on a same task/ file in the solution at the same time?	Cloud architecture provides flexibility to open 2 different actions for the same client in different windows and perform actions simultaneuosly. For instance, bookkeeping can be done on a tab and on another tab payroll can be processed for it's employees. However, two users cannot work on the same file/task at same point of time.	Noted
11.12	How does a user require client input? And what are the ways for a client to provide input?	AO's client side data requests enable clients to provide the required data to complete a task. A few examples are: 1. Data request for collecting financial information, in order to proceed with annual accounts preparation 2. Confirming employee salaries via a data request which is editable to udpate employee information like tax code, salaries etc Once submitted by the client, the accountant has to review it before passing it onto the right module with a click of a button or even request additional info based on queries.	Confirmed
Document & access control			
11.13	How does the system manage document visibility across different client contacts?	Acting Office provides centralised document storage with structured categorisation (folders, tags, bookmarks, important files). From a user's perspective, documents uploaded or automatically saved (e.g., KYC documents) are organised under the relevant client profile and can be managed using features such as notes, bookmarks, and tagging. From a client's perspective, only documents explicitly shared with them through their client portal access will be visible. This ensures that sensitive files remain internal to the practice unless intentionally shared.	Confirmed

11.14	Can access to documents be restricted based on user roles or contact type? Please respond from both a user and client view.	User view: Internal users can restrict document access by applying privacy settings, assigning documents to specific folders, or linking them only to selected tags. Role-based access ensures that only authorised staff members can view or modify sensitive files, while others may have limited rights such as "view only." Client view: For external contacts, access is controlled through the client portal. Only documents marked for sharing are visible to the client. This allows practices to keep compliance files, working papers, or internal notes private while securely providing clients with invoices, agreements, or KYC requests. No access option can be configured for user view.	Confirmed. Document access control between users from the same client is not available out-of-the-box, but can be configured upon request. See conclusion point 2.07.
11.15	Is there a way to track who has viewed or interacted with shared documents?	Yes. The Recent section in the Document tab captures access history, including the date, time, and user who viewed or interacted with a document. This provides a clear audit trail of document usage. Additionally, actions such as moving, renaming, tagging, or deleting documents are logged, ensuring transparency and accountability.	Noted