


Ref	Requirement		
	HEADER		
	ICAEW Technical Accreditation Scheme Audit Testing Software Evaluation		
	AuditBot		
			
	Jul-25		
	© ICAEW. Technical Accreditation Questionnaire		
	CONTENTS		
1	Introduction and Prologue		
2	Issues identified and evaluation conclusion		
	-- GLOBAL REQUIREMENTS:		
3	Access and Security		
4	Data processing and reporting		
5	Usability		
6	SaaS hosting		
7	Audit Testing		

Ref	Requirement	Response	Reviewer Comments
1.	<b>INTRODUCTION AND PROLOGUE</b>		
<b>Introduction</b>			
1.01	The suitability of software for each particular user will always be dependent upon that user's individual requirements. These requirements should therefore always be fully considered before software is acquired. The quality of the software developers or suppliers should also be considered at the onset.		
1.02	<p>Fundamentally, good software should:</p> <ol style="list-style-type: none"> <li>1. Be capable of supporting the functions for which it was designed.</li> <li>2. Provide facilities to ensure the completeness, accuracy, confidentiality and continued integrity of these functions.</li> <li>3. Be effectively supported and maintained.</li> </ol> <p>It is also desirable that good software should:</p> <ol style="list-style-type: none"> <li>4. Be easy to learn, understand and operate.</li> <li>5. Make best practical use of available resources.</li> <li>6. Accommodate limited changes to reflect specific user requirements.</li> </ol> <p>It is essential, when software is implemented, for appropriate support and training to be available.</p>		
<b>Approach to Evaluation</b>			
1.03	The objective is to evaluate a product against a set of criteria developed by the ICAEW to ensure that the software meets the requirements of Good Accounting Software, as laid down in the summary.		
1.04	In order to effectively evaluate the software, a product specialist from the vendor completed the detailed questionnaire and provided it to the ICAEW to examine. The ICAEW's Scheme Technical Manager then reviewed the operation of the various aspects of the software assisted by a member of the vendor's technical staff and checked the answers to confirm their validity. The questions were individually reviewed and commented on and the majority of assessments were confirmed.		
1.05	The Technical Manager discussed the assessment with a member of the vendor's staff in order to clarify any points requiring further information. In the event of disagreement between the supplier and the Technical Manager, the Technical Manager's decision was taken as final and the response changed accordingly.		
1.06	The latest version of the software was used throughout the evaluation.		
1.07	When the evaluation had been completed, a draft copy was sent to the ICAEW Scheme Manager for review before completion of the final report.		

1.08	Key acronyms used throughout the review included: - FFR (First Functional Release) - MFA (multi factor authentication) - SSO (single sign on)		
<b>Prologue: vendor's introduction to their product and comparison</b>		<i>NB: This text has been provided directly by the software vendor and does not form part of the ICAEW's &amp; RSM's evaluation</i>	
1.09	General Overview:	<p>AuditBot has been purpose-built for audit practitioners, with a focus on streamlining fieldwork through automation and enhancing audit quality. The platform is configurable to suit a range of audit firm sizes and workflows, and we work closely with clients to understand their requirements during onboarding.</p> <p>The development team behind AuditBot comprises experienced software engineers and chartered accountants, ensuring a deep understanding of both technical and domain-specific challenges. Our company is ISO27001 certified, and we adopt rigorous development and QA standards, reflecting our commitment to delivering secure, reliable, and high-quality software.</p> <p>AuditBot has been developed specifically to support the core functions of audit fieldwork, including automated data ingestion, analytical procedures, control testing, and working paper generation. The platform is designed to ensure completeness and accuracy in line with recognised audit methodologies. We implement robust data protection measures, including bank-grade AES256 encryption, secure user authentication, and ISO27001-certified hosting, to maintain the confidentiality and integrity of client data.</p>	
1.09 cont.		<p>AuditBot is actively maintained with regular updates based on user feedback, regulatory developments, and technological improvements. Our team provides responsive technical support and comprehensive onboarding, including live training sessions, documentation, and video tutorials, ensuring users can adopt the software effectively.</p> <p>The technical aspects of this questionnaire have been completed by Robbie Lewis, Chief Technology Officer of Digital Planning Limited. Digital Planning is AuditBot's development partner and has led the design, development and deployment of the AuditBot platform. Robbie has an in-depth understanding of both the software architecture and its practical application in the audit domain.</p>	

1.10	Supplier background:	<p>AuditBot was founded in 2024 by audit professionals and tech entrepreneurs. Our mission is to harness the power of machine learning and agentic AI to enhance the quality and efficiency of statutory audits. Over the last two years we have continuously refined our AI models to meet audit practitioners' evolving needs.</p> <p>We welcome the ICAEW's evaluation against established criteria for Good Accounting Software. AuditBot has been developed with a clear focus on quality, integrity, and professional standards. The platform has been designed to align with the expectations of the accountancy profession, and we are confident it meets the ICAEW's criteria in terms of functionality, data integrity, user experience, and ongoing support. We are committed to continuous improvement and view this accreditation process as a valuable benchmark for ensuring our software continues to serve the needs of the profession effectively.</p>	
1.11	Product background and suitability for the user:	<p>AuditBot was developed in collaboration with audit professionals to specifically address the complexities of statutory audits. The platform guides the user through audit testing and generates audit-ready documentation. Each feature aids in aligning with international standards on auditing (ISAs), supporting a robust and defensible audit approach.</p> <p>The platform is designed with usability in mind—intuitive interfaces, contextual help, and streamlined workflows reduce the learning curve. AuditBot is also architected for efficiency, making effective use of system resources, and includes customisable elements to reflect firm-specific procedures or preferences where required.</p>	
1.12	Add-on modules:	None	
1.13	Typical implementation [size]:	<p>AuditBot is offered primarily as a cloud-based offering, making implementation straightforward for audit firms of any size. Implementation typically involves:</p> <p>Initial Setup (1 day) – Configuration, user roles, and security.</p> <p>Data Integration (client by client) – Mapping client data sources (ERP systems, accounting software).</p> <p>User Training (ongoing) – Hands-on workshops for end users and administrators.</p> <p>Firms with 10–500 audit professionals can be on-boarded efficiently, though larger deployments may involve phased rollouts.</p>	
1.14	Vertical applications:	None	
1.15	Server platform and database:	The platform is hosted on Microsoft Azure. All data is encrypted at rest and in transit. We maintain ISO 27001 certification for information security management.	
1.16	Client specification required:	Microsoft Edge or Google Chrome	
1.17	Partner network:	n/a	

Ref	Requirement		
2.	<b>ISSUES AND CONCLUSION</b>		
<b>Highlighted issues</b>			
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)	<b>Question reference</b>	
2.03	As at the date of the software demonstration performed as part of this accreditation process (14 April 2025), this solution was still in it's final stages of development, ahead of formally launching in May 2025.	N/A	
2.04	AuditBot is a solution for a sub-set of fieldwork (an assistive tool to help existing workflows) it is not an end to end audit solution, therefore it is not in a position currently to define all tests required for an audit file and potential customers should ensure they continue to critically evaluate the appropriate tests that should be performed on an audit.	N/A	
2.05	As part of the demo, a demonstration of one test was shown within the AuditBot software "Sales - Transaction Test Completeness Services Setup Test". A further video demo of the "Wages reconciliation test" was shared, which we reviewed independently. Whilst each test is performed slightly differently, core functionality (i.e. define sample sizes, data upload, review of matching / discrepancies of data and working paper generation) is standardised across all tests.  Commentary in tab 7. Audit Testing is however	7.07, 7.08, 7.09	
2.06	Within the FFR, AuditBot is releasing audit tests relating to the P&L only. This includes, purchasing, wages and sales. Balance sheet testing and bespoke testing is planned for future releases.	7.06	
2.07	As at the point of the demonstration on 14 April 2025, there was continued development planned ahead of the FFR on 13 May. This included improvements to access and security (e.g. Microsoft Identity Framework integration including requirements for MFA, passwords minimum length and complexity criteria), initial development of an administration screen and a number of improvements to improve the overall software functionality including allowing further "audit" level documents to be uploaded such as post year end nominal ledger and sales order books which can be used across multiple tests.  We have received attestation from AuditBot that this development has been completed and is confirmed to be included as part of the FFR (although not sighted by RSM as part of this accreditation).	3.04, 3.08, 3.09, 3.10, 3.14, 3.15, 6.08, 7.01, 7.02	

2.08	As AuditBot is a new software to market, the software vendor has a roadmap to develop further functionality and implement improvements to the software for the next 12+ months. Items on the roadmap have not been subject to the accreditation process.	3.01, 3.08, 3.10, 3.21, 3.22, 4.14, 4.21, 4.29, 5.11, 6.27, 6.73, 6.84, 7.13, 7.15, 7.16	
2.09	Regression testing has not been performed - full regression testing is recommended to test system under a code freeze environment pre FFR.	6.74	
2.10	In the FFR, the MFA method will be limited to a one time passcode (OTP) the user's email address. Additional methods (e.g. authenticator apps, OTP via SMS) will be added in future releases (authenticator app planned for Q4 2025). OTPs to email addresses as a MFA method, similarly to mobile/SMS, 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.	3.09	
-			
<b>Evaluation conclusion</b>			
2.11	For the specific use-cases in support of assisting accountancy firms to make effective use of audit testing 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 *		
<b>Disclaimers</b>			
2.12	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.	<b><u>ACCESS AND SECURITY</u></b>		
<b>Access control</b>			
3.01	What security features are included to control access to the application?	<p>Access to the AuditBot platform is controlled through user authentication via email and password. Session management is handled securely via standard browser session protocols, with automatic expiry after 24 hours to minimise the risk of unauthorised access.</p> <p>The platform incorporates role-based access control. Auditor users are assigned roles that determine their level of visibility across audit data. Within each audit firm, an Auditor Admin is designated, with responsibility for account management and user oversight. Auditor users can be restricted to specific audits and tests, ensuring they only access data relevant to their assignments.</p> <p>AuditBot uses AES-256 encryption for data at rest and in transit, and the infrastructure is hosted on ISO27001-certified platforms. Multi-Factor Authentication (MFA) is included as part of FFR, with authenticator app authentication planned for Q4 2025. Single Sign-On (SSO) support is also on the roadmap for future implementation (Q1 2026), in alignment with enterprise security requirements.</p>	<p>Noted</p> <p>See conclusion point 2.08</p>
3.02	Can access to functions be managed via a permissions matrix so users can only see (in menus and other links) and access those areas they are authorised to access?	<p>Yes, AuditBot includes a permissions framework that restricts access to audit data and functionality based on user roles. Auditor users can only view and interact with the specific audits and tests to which they have been assigned. Menu items, links, and functionality within the platform are dynamically adjusted based on each user's access rights, ensuring that users only see the areas of the system relevant to their role and assignments.</p> <p>Each audit firm designates an Auditor Admin, who has broader visibility and is responsible for user management and permissions within their organisation. Non-admin users have restricted access, which can be configured to limit visibility to individual clients or engagements.</p>	Noted
3.03	Is this access to the application managed by:- - Individual user profiles? - User groups or job roles?	<p>Access within the AuditBot platform is primarily managed through defined user roles rather than individually tailored user profiles. These roles determine the level of access and visibility a user has within the application.</p> <p>For example, audit firms designate an Auditor Admin, who can manage users, configure firm-level settings, and access all audit files. Standard Auditor users are assigned to specific audit engagements, and their access is restricted accordingly.</p>	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?	<p>We are currently implementing an administrative screen within the AuditBot platform that enables the Auditor Admin to view and manage all users within their audit firm. This interface will display full user details, including assigned role, engagement type (auditor/client), and a breakdown of the audits and tests each user is authorised to access.</p> <p>This functionality provides a comprehensive overview of user access across the platform and supports effective governance and oversight. While it is not a downloadable report at present, the screen serves the same purpose by consolidating all relevant access information in one place. Future iterations may include export/reporting functionality based on user feedback.</p> <p>Whilst some aspects of an administrative screen were delivered before the FFR (User Settings Page and the Update Payment Method), further development is planned in Q3 2025.</p>	<p>Noted - the administration screen was not live as at the software demonstration performed on 14 April 2025 however we understand the development of this is included in the final sprints ahead of the software release in May 2025.</p> <p>See conclusion point 2.07</p>

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?	<p>Yes, the AuditBot platform dynamically adjusts the display of menu items and in-application features based on the user's role. Auditor Admins and standard Auditor users each see a tailored interface that reflects the permissions associated with their role. This ensures users only view and access functionality relevant to their responsibilities, supporting both usability and data security.</p> <p>Client access is on the roadmap to streamline the client experience</p>	Noted
3.06	Does security allow for access to be limited to: - Read only? - Read/write? - Read/amend/delete?	<p>Currently, access permissions within AuditBot are structured around audit assignments, with users granted full access to the audits and tests they are actively involved in. As such, the system does not presently implement distinct permission levels such as read-only, read/write, or read/amend/delete. However, since users can only see the audits they are assigned to, exposure is already limited by design.</p> <p>The introduction of an Audit Manager role is scheduled for release in July 2025. Introducing more granular permission levels is something we would consider based on user demand, particularly in contexts such as supervisory review, training environments, or restricted collaboration scenarios.</p> <p>Although client access is not planned for the first functional release, this may be included in future releases, and access will be limited to a data upload landing page only.</p>	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?	<p>AuditBot does not expose its data via ODBC or other external report writers. All data access is handled securely within the platform or via tightly controlled API endpoints. There is no direct database-level access for external tools.</p> <p>A limited and secure API-based integration exists between the AuditBot application (hosted on Microsoft Azure and built in .NET Blazor) and our WordPress-based commercial website (hosted with Cloudways). This integration is used exclusively to synchronise essential account information such as name, email, password, and payment method status to maintain a consistent user identity across both environments.</p> <p>All API communications are encrypted in transit, and no user data is made accessible outside of the controlled application environment. Access controls are enforced consistently across both platforms to ensure data protection and alignment with each user's permissions.</p>	Noted
3.08	Does the system security integrate with Microsoft's Active Directory or other tools that provide a single sign-on?	<p>AuditBot does not currently integrate with Microsoft Active Directory or other Single Sign-On (SSO) providers. However, SSO functionality is on our development roadmap and is planned for a future release (Q1 2026). This will enable integration with common identity providers, including Microsoft Entra ID (formerly Azure Active Directory), in line with enterprise security expectations and to streamline access management for larger audit firms.</p> <p>We recognise the importance of federated identity and role-based provisioning and will ensure that access controls and security auditing are aligned with these capabilities once implemented.</p> <p>The Microsoft Identity Framework integration will be used as the primary framework for access security. This will include MFA and enhanced requirements for password protection including length, complexity and history. This integration is planned ahead of the first functional release in May 2025.</p>	<p>Noted - this was not live as at the software demonstration performed on 14 April 2025 however we understand implementation of the Microsoft Identity Framework (which includes MFA) is included in the final sprints ahead of the software release in May 2025.</p> <p>See conclusion point 2.07 &amp; 2.08</p>



3.09	Does the system provide multi-factor authentication (MFA)?	<p>Multi-Factor Authentication (MFA) is not currently available within the AuditBot platform however will be included as part of the FFR.</p> <p>Once released, MFA will enhance account security by requiring a second verification method in addition to the standard email and password login. The implementation will align with best practices for authentication security and is intended to meet the expectations of audit firms and regulatory bodies for protecting sensitive financial data.</p> <p>The Microsoft Identity Framework integration will be used as the primary framework for access security. This will include MFA and enhanced requirements for password protection including length, complexity and history. This integration is planned ahead of the first functional release in May 2025.</p> <p>In the FFR, the MFA method will be limited to a one time passcode (OTP) the user's email address. Additional methods (e.g. authenticator apps, OTP via SMS) will be added in future releases (authenticator app planned for Q4 2025).</p>	<p>Noted - this was not live as at the software demonstration performed on 14 April 2025 however we understand implementation of the Microsoft Identity Framework (which includes MFA) is included in the final sprints ahead of the software release in May 2025.</p> <p>OTPs to email addresses as a MFA method, similarly to mobile/SMS, 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.</p> <p>See conclusion point 2.07 &amp; 2.10</p>
<b>Passwords and access logs</b>			
3.10	Is access to the software controlled by password?	<p>Yes, access to the AuditBot platform is currently controlled by a secure email and password login system. Passwords are encrypted using industry-standard hashing algorithms and are never stored in plain text. Users are required to create a strong password upon account setup, and the system supports secure password reset functionality.</p> <p>We are also in the process of enhancing access controls through the planned introduction of Multi-Factor Authentication (MFA) ahead of release and Single Sign-On (SSO) in Q1 2026, to further strengthen authentication mechanisms.</p>	<p>Confirmed - email and password login screen.</p> <p>Noted - MFA was not live as at the software demonstration performed on 14 April 2025 however we understand implementation of the Microsoft Identity Framework (which includes MFA) is included in the final sprints ahead of the software release in May 2025.</p> <p>See conclusion point 2.07 &amp; 2.08</p>
3.11	Does each user have a separate log on (user id)?	Yes, each user on the AuditBot platform is assigned a unique user ID, linked to their individual email address. This ensures that access is securely personalised, auditable, and role-specific. Shared accounts are not supported, and all actions within the system can be attributed to a specific user, which supports accountability and audit trail integrity.	Noted
3.12	If there is no password facility please state how confidentiality and accessibility control is maintained within the software?	n/a	n/a
3.13	Are passwords masked for any user logging in?	Yes, all password fields within the AuditBot platform are masked using standard HTML password input fields. This ensures that passwords are not visible on screen during entry, in line with	Noted

3.14	Is password complexity available and enforced?	<p>Password complexity requirements are not currently enforced within the AuditBot platform. However, the introduction of configurable password policies — including minimum length and complexity criteria — is on our development roadmap. This enhancement will align with best practices in authentication security and support compliance with firm-level and regulatory standards.</p> <p>Automatic locking out of users after a number of unsuccessful attempts will be in place by the first functional release.</p> <p>The Microsoft Identity Framework integration will be used as the primary framework for access security. This will include MFA and enhanced requirements for password protection including length, complexity and history. This integration is planned ahead of the first functional release in May 2025.</p>	<p>Noted - this was not live as at the software demonstration performed on 14 April 2025 however we understand implementation of the Microsoft Identity Framework (which includes enhanced complexity requirements) is included in the final sprints ahead of the software release in May 2025.</p> <p>See conclusion point 2.07</p>
3.15	How many previous passwords are retained / the password history?	<p>AuditBot does not currently retain previous passwords or enforce a password history policy. However, we recognise the value of preventing password reuse as part of a broader security framework, and we would consider adding this functionality to our development roadmap in response to client or regulatory requirements.</p> <p>The Microsoft Identity Framework integration will be used as the primary framework for access security. This will include MFA and enhanced requirements for password protection including length, complexity and history. This integration is planned ahead of the first functional release in May 2025.</p>	<p>Noted - this was not live as at the software demonstration performed on 14 April 2025 however we understand implementation of the Microsoft Identity Framework (which includes history requirements) is included in the final sprints ahead of the software release in May 2025.</p> <p>See conclusion point 2.07</p>
3.16	Are passwords encrypted?	<p>AuditBot uses ASP.NET Core Identity for user authentication across the platform. In line with best practices, user passwords are not stored in plain text or encrypted directly. Instead, they are securely hashed using PBKDF2 (Password-Based Key Derivation Function 2) with HMAC-SHA256.</p> <p>This approach includes salting and multiple iterations, making it computationally infeasible to reverse the hash and retrieve the original password. This ensures strong protection of user credentials in the event of a data breach and aligns with industry standards for credential security.</p>	Noted
3.17	<p>Are users automatically logged off after a pre-set idle time?</p> <p>- Can the time period be changed?</p> <p>- Can any information be viewed without being logged in, including after logging off, if so what information?</p>	<p>Users are currently logged out automatically after 24 hours through browser session expiry. At present, the idle timeout duration is not configurable by the user or administrator. However, we recognise the security benefits of shorter, inactivity-based session timeouts and would be open to incorporating this feature into our development roadmap based on client demand.</p> <p>Once a user is logged out, either manually or through session expiry, no application data or functionality is accessible. All sensitive audit content and user-specific information is securely protected behind the login process, and no residual data remains viewable in the browser following logout.</p>	Noted
<b>Deletion of transactions</b>			
3.18	Is it possible to delete a transaction?	<p>In the context of AuditBot, “transactions” are interpreted as audit data, uploaded documents or test results within the application. The system does not allow for hard deletion of this data. Instead, a soft-delete mechanism is used: when an item is deleted by a user, it is flagged as deleted within the database and removed from visibility in the application interface and calculations.</p> <p>This approach ensures that no audit data is permanently removed, supporting the integrity of the audit trail and allowing for full traceability. Soft-deleted records remain available for administrative or compliance review if required, aligning with professional standards around audit evidence and documentation retention.</p>	<p>Noted - it is important to note that AuditBot is not an end to end audit solution and therefore the quality and completeness of an audit file will rely on the audit methodology and professional scepticism of the audit firm conducting the audit.</p>
3.19	If so, then how are deletions controlled by the system?	See above.	Noted
3.20	Are deleted transactions retained in the audit trail (see below) and denoted as such?	See above.	Noted

Audit trails			
3.21	Does the system have an audit trail (log) which records all changes to transactions in the system?	<p>AuditBot does not currently include a user-facing audit trail feature that logs all changes to transactions within the system. However, we recognise the importance of comprehensive audit logging — particularly in the context of financial data integrity — and this capability is on our development roadmap. This is planned for release in Q3 2025.</p> <p>At present, many actions and data changes can be traced retrospectively through the underlying database using custom queries, enabling internal review where necessary. Future updates will include a structured, queryable audit log to record key user actions such as data creation, updates, deletions (via soft-delete), and assignment changes, with timestamps and user attribution.</p>	<p>Noted</p> <p>See conclusion point 2.08</p>
3.22	Does this log also record any system error messages and/or any security violations?	<p>Yes, all unhandled exceptions and system-level errors within the AuditBot platform are currently logged using Azure Application Insights. This enables the development team to monitor, investigate and resolve issues promptly. Logs include exception details, stack traces, and contextual information to support root cause analysis.</p> <p>While security violation logging is not yet fully implemented, we plan to expand our monitoring capabilities to include failed login attempts, unauthorised access attempts, and other relevant security events. This feature is planned for release in Q3 2025. These enhancements are part of our roadmap to strengthen operational oversight and align with best practices in application security monitoring.</p>	<p>Noted</p> <p>See conclusion point 2.08</p>
3.23	Is it possible to turn off or delete the audit trail?	No	Noted
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?	<p>AuditBot does not currently implement a formal audit log that assigns system-generated sequential reference numbers to each user transaction. However, key metadata such as unique record identifiers, creation/modification timestamps, and user attribution are stored at the database level for core application data.</p> <p>In addition, all unhandled exceptions and system-level events are captured by Azure Application Insights. These logs include detailed information such as timestamps, user identifiers (where available), session context, and error diagnostics, providing useful traceability for operational and debugging purposes.</p> <p>A structured audit log feature is planned for future development. This will incorporate sequential transaction IDs, full timestamping, and user attribution to support comprehensive audit trail functionality aligned with professional and regulatory expectations.</p>	<p>Noted - sequential unique reference numbers are unlikely to be necessary unless the audit conclusion is highly material or there is a significant issue with the audit data (e.g., data loss or scrambling). As long as transactions can be identified in some manner, this should suffice for traceability and transaction identification.</p>
3.25	Are all master file changes recorded in the audit trail?	<p>AuditBot does not generate or maintain a single, consolidated master audit file. Instead, it produces structured outputs — including Excel worksheets for each audit test — which auditors can review and incorporate into their own working papers and master files as appropriate.</p> <p>As the master file is assembled and maintained independently by the audit firm, it is the responsibility of the firm to retain an appropriate audit trail for any changes made to that document. AuditBot ensures the integrity and traceability of the data it generates, but it does not track downstream modifications to exported files made outside of the system.</p>	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?	<p>Yes, AuditBot operates in full alignment with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Our privacy practices are outlined in our Privacy Policy, which is publicly accessible via our website.</p> <p>On our commercial website (WordPress), we implement a GDPR-compliant cookie consent banner allowing users to manage preferences regarding analytics and marketing cookies. The AuditBot application itself does not currently utilise any non-essential cookies, but if such functionality is introduced in future, appropriate consent mechanisms will be implemented.</p> <p>Beyond cookie management, we apply core GDPR principles across the platform:</p> <p>Lawful Basis: Personal data is processed under clear legal bases, including contract fulfilment, legitimate interest, legal obligation, and consent where applicable.</p> <p>Security: Data is stored on ISO27001-certified infrastructure with AES-256 encryption in transit and at rest. We enforce role-based access controls and conduct regular security reviews.</p> <p>Data Subject Rights: Users can exercise rights to access, rectify, erase, or restrict their data, and can contact our Data Protection Officer via the published channels.</p>	Noted
3.26 cont.		<p>Retention: Personal data is retained only as long as necessary to meet legal and operational requirements.</p> <p>AuditBot does not share personal data with third parties unless necessary for service delivery or to meet regulatory obligations, and all transfers are governed by appropriate data protection agreements.</p>	
3.27	Describe your use of sub-processors if any?	<p>AuditBot makes limited use of sub-processors to support specific functionality within the platform. We use Azure Document Intelligence (a Microsoft Azure service) to extract structured data from documents uploaded by users for the purpose of automated audit testing. This enables intelligent parsing and significantly reduces manual data entry.</p> <p>All data processed by Azure Document Intelligence remains within the UK South Microsoft Azure datacentre, which is ISO27001-certified and compliant with UK GDPR. Data is encrypted both in transit and at rest, and is subject to Microsoft's standard contractual terms for sub-processing.</p> <p>No other sub-processors are currently used for application functionality. Should additional sub-processors be introduced in future, they will be subject to appropriate due diligence, contractual safeguards, and notification procedures in line with our privacy policy and data protection obligations.</p>	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?	<p>We are currently developing a public-facing knowledge base that will include detailed information on data backup and recovery processes.</p> <p>Data within the system cannot be 'hard deleted', ensuring recovery and backup capabilities. In the event of a server failure, a server switch can be executed at the backend to maintain continuity.</p>	Noted
3.29	How often are backups taken and to what point can restores be done?	<p>The AuditBot platform currently performs full database backups on a daily schedule. These backups are securely stored within Microsoft Azure's UK South datacentre and benefit from encryption at rest and in transit, as well as the resilience features of Azure's managed backup services.</p> <p>As the platform transitions into active use with live clients, we plan to increase the backup frequency to hourly to ensure shorter recovery windows and improved data protection. The underlying infrastructure supports flexible backup intervals, allowing us to tailor the frequency to operational needs and client expectations.</p>	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).	<p>AuditBot does not currently include automated, user-initiated recovery procedures such as transactional rollbacks within the application itself. However, in the event of a software failure or critical incident, our development team can perform a manual recovery by restoring the database from the most recent backup and relaunching the application on a clean server instance.</p> <p>Backups are securely stored within Microsoft Azure and can be restored to a known good state. This process enables us to roll back to the last completed backup, minimising disruption and data loss.</p> <p>As part of our operational readiness, this recovery process will be practised on a quarterly basis to ensure familiarity, reduce recovery time, and maintain confidence in our disaster recovery plan.</p>	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?	<p>Within AuditBot, audit tests are processed as batch operations. Documents and user inputs are ingested and processed together, and results are only committed once the full test completes successfully. If a failure occurs part way through the process, no partial data is saved, and the test would need to be re-run in full. This ensures data integrity and prevents incomplete or inconsistent outputs from being stored.</p> <p>To support accuracy and user control, the platform includes a dedicated review step for handling matching errors between scanned documents. During this step, users can review any discrepancies identified by the system and resolve them by overriding scanned values. This includes the ability to correct values that may have been misread by the Azure Document Intelligence engine. These override capabilities help ensure high data quality while still maintaining a streamlined batch processing approach.</p>	Noted

3.32	What features are available within the software to help track down processing problems?	<p>AuditBot includes several features to help users identify and resolve processing issues during audit test workflows. A key part of this is the document matching and review step, which highlights discrepancies or extraction errors encountered during the document scanning process. Users are able to override system-detected values where necessary — for example, correcting misread amounts — before proceeding to the results stage. This provides a clear and interactive mechanism for resolving problems before they impact outputs.</p> <p>In the event of an unexpected system error, unhandled exceptions are automatically logged using Azure Application Insights. This enables the development team to monitor and trace issues using detailed error reports, stack traces, and contextual information. This infrastructure supports fast diagnosis and resolution of backend processing problems outside the user interface.</p> <p>Together, these user-facing and developer-facing tools provide a comprehensive framework for identifying, understanding, and resolving issues during audit processing.</p>	Noted
------	---	--	-------

Ref	Requirement	Response	Reviewer Comments
4.	<b>DATA PROCESSING AND REPORTING</b>		
<b>Input and validation of transactions</b>			
4.01	Is data input controlled by self-explanatory menu options?	<p>Yes, data input in AuditBot is guided by self-explanatory menu options and clearly structured forms. We have placed significant emphasis on user experience (UX), following best practices in interface design to ensure the platform remains intuitive and accessible despite the inherent complexity of audit processes.</p> <p>Tooltips, field labels, and layout decisions have all been carefully considered to streamline navigation and reduce input errors.</p> <p>The interface has undergone several iterative improvements based on user feedback.</p>	<p>Noted - most of the user-facing system has been sighted as part of the software demonstration performed on 14 April 2025. The user experience (UX) appears intuitive and adheres to best practice interface design principles. However, it is important to note that not all functionality has been fully observed, including all the testing features.</p>
4.02	Are these menus user/role-specific?	<p>Yes, menus within the AuditBot platform are tailored according to user roles. Auditor Admins, standard Auditor users, and Client users each see a different set of menu options, reflecting their permissions and responsibilities within the system.</p> <p>This role-based interface ensures that users only see the data and functionality relevant to their role.</p> <p>NB: client user access will not be included in the launch of the software in May 2025.</p>	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?	<p>Yes, the creation and amendment of standing data such as client details and audit configurations can be managed directly within the AuditBot platform using menu options and dialogue boxes. These actions do not require any back-end configuration or technical involvement, allowing users — particularly Auditor Admins — to make changes quickly and easily via the application interface.</p> <p>Functionality for managing user assignments through the interface is currently in development. Once complete, this will allow Auditor Admins to assign team members to specific audits directly through the platform, further enhancing administrative efficiency and access control.</p>	Confirmed
4.04	Does the software provide input validation checks such as: - [account] code validation? - reasonableness limits? - validity checks?	<p>Yes, AuditBot includes a range of input validation mechanisms to ensure data accuracy and consistency:</p> <p>Account Code Validation: The platform supports importing account codes from IRIS accounting software, with integrations for CaseWare and CCH scheduled for release later this year. We are also implementing a connection to Merge.dev, which will allow integration with a wide range of online accounting platforms. Imported account codes are validated for uniqueness and structure during the import process.</p> <p>Reasonableness Limits: Each test in AuditBot includes a review stage where discrepancies or unexpected results are flagged and resolved. We are currently enhancing this further by introducing the Trial Balance as a central audit-level document, which will serve as a reference point across multiple tests, allowing automated checks for consistency and accuracy.</p> <p>Validity Checks: Input fields across the platform are subject to appropriate validation rules. Numeric and decimal fields enforce correct formats, phone numbers use input masks, and email fields require valid syntax. Required fields are enforced where applicable to ensure completeness of audit data.</p> <p>These validation features help maintain the quality and reliability of the audit evidence generated within the platform.</p>	<p>Noted - as at 14 April 2025:</p> <p>Account Code Validation - noted however, not sighted and not planned for First Functional Release. Understand that is this planned for future releases.</p> <p>Reasonableness Limits - sighted 14 April 2025 that all variances are flagged once AuditBot has reviewed the source data. Note that this does not consider a materiality limit, with any and all variances flagged.</p> <p>Validity Check - noted however, not sighted.</p>

4.05	What control features are within the software to ensure completeness and accuracy of data input?	<p>AuditBot includes several control features designed to ensure completeness and accuracy of data input:</p> <p>Structured Workflows: Each test follows a defined structure, guiding the user through required inputs step by step. This reduces the likelihood of missing or incomplete data.</p> <p>Field-Level Validation: Inputs are validated at the field level with data type enforcement (e.g. decimal formatting, input masks for phone numbers, and syntax checks for email addresses). Required fields are clearly marked and enforced before users can proceed.</p> <p>Test Completion Checks: Each audit test includes a review or “checking” stage, where inconsistencies or missing elements can be identified and resolved before the test is marked as complete.</p> <p>Centralised Data Reference: We are in the process of making the Trial Balance an audit-level document, allowing it to serve as a reference point for multiple tests. This will provide additional data integrity checks across the platform.</p> <p>Controlled Imports: Account codes and trial balances imported from external accounting platforms are validated for structure and uniqueness, supporting accuracy at the point of ingestion.</p>	<p>Noted - as at 14 April 2025:</p> <p>Structured Workflows - sighted through cash and wages testing demo as at 14 April 2025. Note that have not sighted 100% of tests, therefore cannot confirm for all.</p> <p>Field-Level Validation - sighted through cash and wages testing demo as at 14 April 2025. Note that have not sighted 100% of tests, therefore cannot confirm for all.</p> <p>Test Completion Checks - noted.</p> <p>Centralised Data Reference - was not sighted as at 14 April 2025, as functionality is planned for future releases.</p> <p>Controlled Imports - noted.</p>
4.06	How does the software ensure uniqueness of the input transactions? (i.e. to avoid duplicate transactions)	AuditBot collects and matches data together to create auditable transactions. Duplicate entries would be ignored during the matching process or, if included in an audit test would lead to validation where inflated totals would not match.	Noted
4.07	Is data input by users validated by scripts or routines in the browser, or other client software, before transmission to the server?	Yes, data input within AuditBot is validated on the client side using built-in validation routines provided by the Blazor framework. These scripts enforce input formats, required fields, and basic data constraints (e.g. valid email addresses, numeric input, character limits) before any data is transmitted to the server.	Noted
4.08	Is data input by users validated by routines running on the server before data files are updated?	<p>Yes, all user input in AuditBot is validated on the server side before any data is written to the database. This includes enforcing data types, required fields, and business rules to ensure that only valid and complete data is accepted.</p> <p>Server-side validation acts as a second layer of protection, complementing client-side checks and helping to prevent invalid or potentially harmful input.</p>	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?	<p>Yes, AuditBot includes input validation mechanisms that restrict both the length and content of data entered in input fields.</p> <p>Maximum Lengths: All input fields are subject to defined maximum lengths, both on the client side (via Blazor form controls) and on the server side, ensuring that data cannot exceed expected limits. This prevents issues such as buffer overruns or unexpected data truncation.</p> <p>Character Validation: Input fields are validated to restrict unaccepted or potentially unsafe characters, such as semicolons, where appropriate.</p>	Noted
4.10	Are input errors highlighted?	Yes, input errors are clearly highlighted within the AuditBot platform to guide users in correcting them.	Noted - errors were not viewed within demo as at 14 April 2025 (a negative testing
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, input errors are rejected at the point of entry and an on-screen error message is displayed immediately. The AuditBot platform uses in-form validation to inform users of the specific issue, such as a missing required field or invalid data format.	Noted - see above



4.12	Are responses to erroneous data input clear so that they do not lead to inappropriate actions?	Yes	Noted - see above
4.13	Does the software have an automatic facility to correct/reverse/delete transactions?	<p>Yes, AuditBot provides users with the ability to manage and revise input data as needed. Uploaded documents can be removed or replaced at any point, including after test calculations have been run. This allows auditors to update or correct supporting evidence without needing to restart the entire audit process.</p> <p>Additionally, any test within an audit can be repeated if necessary. This gives audit teams flexibility to re-perform procedures when updated information becomes available or when revisions are required.</p>	Noted
4.14	If yes, are these logged in the audit trail?	<p>Currently, changes such as the removal or replacement of documents and the repetition of audit tests are not logged in a formal audit trail within the platform. However, AuditBot uses a soft-delete model, meaning removed items are not permanently deleted from the database. This allows for the possibility of retrospective analysis through internal queries if needed.</p> <p>We recognise the importance of maintaining a comprehensive audit trail and have plans to implement structured logging of key actions — including document replacement, test re-runs, and data changes — in a future release. This feature is planned for Q3 2025.</p>	<p>Noted - have not sighted soft delete functionality as at 14 April 2025. It is important to note that AuditBot is not an end to end audit solution and therefore the quality and completeness of an audit file will rely on the audit methodology and professional scepticism of the audit firm conducting the audit.</p> <p>See conclusion point 2.08</p>
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?	<p>AuditBot includes a dedicated review stage within every audit test where all values used in test calculations are presented to the user for confirmation. This stage acts as a validation checkpoint, ensuring that any inconsistencies or missing inputs are identified and resolved before the test is executed.</p> <p>While the system does not use transactional rollback in a traditional database sense, the structured workflow and pre-test review process serve to maintain the integrity and completeness of each audit test.</p>	Noted
4.16	Are messages provided to users clearly explaining whether the data entry or file upload has been processed successfully or not?	Yes	Confirmed
<b>Import and export of data</b>			
4.17	Can files/attachments be uploaded and stored against any transaction?	Yes	Confirmed
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	Noted
4.20	Explain how the system validates imports into the system and what happens to any import which fails?	<p>AuditBot supports the import of CSV, XLSX, and PDF files, which are validated through a combination of automated checks and human-led review. Established and well-maintained code libraries are used to parse these file types, with comprehensive error handling in place to identify malformed or unreadable content during the import process.</p> <p>The application presents a preview of imported documents, allowing users to visually confirm that the values have been captured correctly. This side-by-side preview with the captured values serves as a key validation step before any test calculations are performed.</p> <p>If an import fails — due to format issues, missing values, or unreadable content — the system prevents further progression and provides appropriate feedback to the user, prompting them to resolve the issue before continuing.</p>	Noted - whilst we sighted a document upload, this did not fail so cannot confirm this functionality.

4.21	Are imported /interfaced transactions detailed in the audit trail? <i>[See also 3.27]</i>	<p>At present, imported transactions and documents within AuditBot are not recorded in a formal, user-facing audit trail. However, the system uses a soft-delete model and stores metadata related to uploaded and imported files, including timestamps and file details, which can be accessed for internal review if needed.</p> <p>The implementation of a structured audit trail that logs key user actions — including imports, document replacements, and test executions — is on our development roadmap. This feature is planned for release in Q3 2025.</p>	<p>Noted</p> <p>See conclusion point 2.08</p>
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?	<p>Yes, AuditBot supports data export from multiple areas of the system in widely used formats. The primary export format is Excel (XLSX), which is used to generate working papers for individual audit tests.</p> <p>It is also possible to download documents that have been uploaded to an audit if you have access to it.</p>	Noted
<b>Data processing</b>			
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)?	<p>Yes, AuditBot ensures that tasks are performed in the correct sequence through a structured workflow model. Each audit test follows a defined process that includes document upload, data extraction, value review, and a final test execution stage. Users are required to complete each stage before progressing, ensuring that no test is finalised using incomplete or unverified data.</p> <p>The platform does not operate on a traditional period-close or month-end basis, as found in accounting software. However, it enforces sequencing and data dependency within the audit workflow — for example, discrepancies must be resolved during the review stage before a test can be completed.</p>	Confirmed
4.24	Does the software provide automatic recalculation, where appropriate, of data input? (e.g. VAT)	Yes, AuditBot performs automatic recalculations where appropriate throughout the audit workflow. Once source documents are uploaded and validated, the platform extracts relevant values and automatically runs predefined test calculations based on those inputs.	Noted
4.25	Is a month/period-end routine required to be undertaken?	No	Noted
4.26	Is it possible to delete accounts if the balance is Nil but transactions have been recorded against the code?	n/a	n/a
4.27	What is the size and format of reference numbers and descriptions within:- - Ledgers? - Stock? - Currencies?	n/a	n/a
4.28	How does the software guard against/warn about duplicate account numbers on set up?	n/a	n/a
4.29	How does the software enable the traceability [from, to and through the accounting records] of any source document or interfaced transaction?	AuditBot is actively developing features to enhance end-to-end traceability of source documents and transactions throughout the audit process. Our roadmap for Q1 2026 includes the ability to inspect and navigate full transaction flows. Intuitive UI will allow simple navigation between related documents to visualise the full transaction.	Noted - as at 14 April 2025 this functionality has not been sighted. Understand that it is currently on the roadmap for 2026. Not a critical requirement for FFR.
4.30	What drill down/around functionality is available within the software?	AuditBot currently supports a structured workflow for each audit test, allowing users to view the source document, extracted data, and test logic within a single interface. This creates a form of drill-down functionality, enabling users to trace back from test outputs to the original supporting evidence.	Confirmed
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?	AuditBot is designed primarily for the analysis of historical financial data in the context of audit engagements. As such, most standing information — such as client details, trial balances, and supporting documents — is static for the duration of an audit and does not require frequent updates.	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)?	<p>AuditBot does not use a separate in-built report generator or third-party reporting engine. Instead, reporting is integrated directly into the application interface, with most outputs displayed as structured web pages that guide the user through each audit test and its results.</p> <p>At the conclusion of each test, a formal working paper is generated and exported in XLSX format. These exports are produced using an established code library.</p>	Confirmed - reporting not part of the platform but this is appropriate based on the platform use case
4.33	Is the report writer based on a standard SQL-type approach and is it flexible and easy to use?	n/a	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	n/a
4.35	Is a comprehensive data dictionary provided to aid field selection?	n/a	n/a
4.36	Does the system provide a library of reports and templates which can be amended, saved and re-run?	n/a	n/a
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?	n/a	n/a
4.39	Can regular reports be added to user menus in the appropriate area of the system?	n/a	n/a
4.40	Does the system support the production of on demand (interactive) and scheduled batch reports?	No	Noted

Ref	Requirement	Response	Reviewer Comments
5.	<b>USABILITY</b>		
<b>Ease of use</b>			
5.01	Does the solution provide a multi-language user interface?	No	Confirmed
5.02	Does the system allow for customizable branding and UI (e.g. corporate colour palate, upload company logo, etc)?	Not yet, we have plans to support white labelling.	Confirmed
5.03	Does the system have a similar look and feel and overall and consistency between screens and modules?	Yes	Confirmed
5.04	Is data entry easily repeated if similar to previous entry?	No	Noted
5.05	Does the software prevent access to a record while it is being updated?	No	Noted
5.06	Is there locking at file or record level?	n/a	n/a
5.07	Does the software allow for the running of reports whilst records are being updated?	No	Noted
5.08	Can timestamps or user comments be added to transactions?	Comment boxes are available for user comments to be added.	Confirmed
5.09	Is there the ability to store preferences and default values on a per-user basis. e.g. department/team/user?	<p>AuditBot supports per-audit customisation through a feature called "Aliases". This allows auditors to tailor document scanning behaviour based on terminology specific to the client or engagement.</p> <p>For example, if a company uses a non-standard label such as "PO Ref" instead of "Order Reference," the auditor can configure an alias so that the scanning engine correctly identifies and extracts the relevant value across similar documents throughout the audit. These aliases are remembered within the audit context, allowing for consistent data extraction and reduced manual correction.</p>	Noted
5.10	Does the system have the ability to provide user-defined fields with associated validation of data input?	No, all fields are defined by AuditBot	Noted
5.11	Can the system provide users with reminders and notifications e.g. workflows?	<p>Yes, AuditBot currently uses email notifications to keep both auditors and clients informed throughout the audit process. Notifications are triggered by key events, such as document uploads, assignments, or updates requiring attention, helping to maintain engagement and ensure timely responses.</p> <p>We are also developing an in-app notification system, which is on our roadmap. This will enable real-time alerts and task reminders directly within the platform interface, supporting a more seamless and responsive workflow experience for users. This feature is planned for release in Q4 2025.</p>	<p>Noted</p> <p>See conclusion point 2.08</p>
5.12	If the system provides workflows, does it have functionality to substitute/delegate authorisations?	No	Noted - as AuditBot is not an end to end solution this is not material.
5.13	Describe the tools and features available for a power user to make configuration changes such as amending a workflow.	n/a	n/a
5.14	Is there the ability for users to define and configure layouts of letters and forms?	No	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?	No	Noted
5.17	Can the system store menu option 'favourites' on a per user basis?	No	Noted
5.18	Can a user open multiple windows accessing the same or different modules of the system?	No	Noted
5.19	Can more than one software function be performed concurrently?	No	Noted

User documentation and training			
5.20	Confirm whether a user manual / instructions is provided and how this is distributed?	We are building a public-facing knowledge base which will cover all aspects of using the application. Links to this will be provided within the application from the FFR.	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?	We are using Atlassian Confluence to host the knowledge base. It will include all of the items listed in the question.	Noted
5.22	Is context-sensitive help available within the system?	Tooltips and notes are provided throughout the application.	Noted
5.23	Is the manual and/or help editable by the user (subject to the permissions matrix)?	No, but we have the ability to allow wiki style editing and user contributions in the knowledge base if needed.	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)?	Documentation is available via a public-facing knowledge base website.	Noted
5.25	Please detail the training options available?	Provided by AuditBot to Firm Champions at the start of the engagement. The exact level of training required is still to be determined as the product has yet to be tested by multiple firms in multiple environments.	Noted
5.26	Who provides training: - Software House? - VAR?	Software house	Noted
Support and maintenance			
5.27	How is the software sold: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	AuditBot is owned and licensed by AuditBot Limited.	Noted
5.28	How is the product supported: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	Support is provided by AuditBot Limited and Digital Planning Limited via a ticketing system and tiered support teams.	Noted
5.29	Do VARs have to go through an accreditation process?	No VAR's	Noted
5.30	Is the software sold based upon number of named users or a number of concurrent users?	Audits are sold individually at a fixed rate.	Noted
5.31	The supplier should detail the support cover options available, covering: - The hours provided? - Associated costs? - The global regions covered?	Users can file tickets that will be responded to within 48 hours. Support is offered on a customer by customer basis.	Noted
5.32	Detail the process by which customers raise support requests and how these can be viewed/managed?	Support is provided by AuditBot Limited and Digital Planning Limited via a ticketing system and tiered support teams.	Noted
5.33	Please note the methods of support available: - Telephone? - Internet chat? - Remote access to customer workstation? - Other, please specify?	Email, Ticket System, Telephone	Noted
5.34	Do you offer service credits for failure to meet performance around SLA and uptime (if	No	Noted
5.35	What is your escalation path for tickets which have not been resolved within a reasonable time?	We will use a tiered support teams (Level 1, 2, 3) with a structured escalation process.	Noted
5.36	How often are general software enhancements provided?	AuditBot is in continuous development. Releases are currently weekly but will likely shift to monthly after launch.	Noted
5.37	Will they be given free of charge?	Yes	Noted
5.38	How are enhancements and bug fixes provided to customers?	Via our changelog, which can be found in the knowledge base.  There is a dedicated development stream that will manage defect management and bug fixes once the software has been released. This will included a tiered approach.	Noted

5.39	Is “hot line” support to assist with immediate problem solving available?	No. Users can file tickets that will be responded to within 48 hours. Support is offered on a customer by customer basis.	Noted
5.40	If so, is there an additional cost involved?	n/a	n/a
5.41	At what times will this support be available?	n/a	n/a
<b>Integration and www facilities</b>			
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)?	n/a	n/a
5.43	Are they integrated on real time basis or batch basis?	n/a	n/a
5.44	Can the software be linked to other packages e.g. word processing, graphics, financial modelling, to provide alternative display and reporting facilities?	No	Noted
5.45	Can definable links to spreadsheets be created?	No	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.	All data is stored in Microsoft Azure services using encryption at rest and during transmission.	Noted
5.47	Can documents be scanned into a secure repos	All documents are stored in Microsoft Azure services using encryption at rest and during transmission.	Noted
5.48	Does the system provide data migration tools for transactional and master data sets (e.g. employees customers, suppliers, journals, invoices).	No	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?	None	Noted
5.50	Does the system support mobile working?	It is possible to access the website on mobile but we have not yet fully optimised the interface for mobile screens.	Noted

Ref	Requirement	Response	Reviewer Comments
6.	<b>SaaS HOSTING</b>		
	<b>This evaluation covers the system but not the method by which it is delivered and/or contracted for. Potential users need to satisfy themselves on the security and disaster recovery aspects and licensing of the online system and any data protection issues of their own and customer/supplier</b>		
<b>Data centres and customer data</b>			
6.01	Please confirm the cloud hosting provider used to host the platform and which region(s) are used.	AuditBot is delivered as a SaaS (Software as a Service) solution and is hosted on Microsoft Azure, using data centres located in the UK South region. These facilities are owned and operated by Microsoft and are ISO27001, ISO27017, and ISO27018 certified.	Noted
6.02	Does the customer get a choice of the jurisdiction in which their data resides?	Not currently, all data and documents are stored in Microsoft's UK South datacentre.	Noted
6.03	What certification(s) do you or your platform operators hold relating to your data centres and your business operations?	<p>AuditBot is hosted on Microsoft Azure, which holds a comprehensive set of certifications for its data centre operations, including:</p> <p>ISO/IEC 27001 – Information Security Management</p> <p>ISO/IEC 27017 – Cloud Security</p> <p>ISO/IEC 27018 – Protection of Personal Data in the Cloud</p> <p>SOC 1, SOC 2, and SOC 3 – Service Organisation Controls</p> <p>PCI-DSS – Payment Card Industry Data Security Standard</p> <p>Cyber Essentials Plus – For services hosted in UK government-compliant regions</p>	Noted
6.04	Do you or your platform operator have an SSAE16 (System and Organization Controls) report available?	No	Noted
6.05	What are the physical controls over the:- - Premises? - Fileservers? - Communications equipment?	You can read more about physical controls of Microsoft Azure datacentres here: <a href="https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security">https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security</a>	Noted
6.06	Is the space in this/these data centre(s) shared with any other companies?	Yes	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?	Test data and documents for AuditBot audit clients are stored together but separated using logical security.	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?	The separation of data is controlled throughout the application using logical security, in addition to row Level Security (RLS) in the database to further enhance separation of data. Data and documents belong to tests within audits. Users can only access data or documents if they have the necessary permissions for that audit.	<p>Noted - User access is role based and defined by the Audit Admin at Audit file creation through the administrative screen. As at 14 April 2025 have not sighted administrative screens. However, understand that it is planned for the first functional release.</p> <p>See conclusion point 2.07</p>

6.09	What controls are in place to prevent users from one customer/company accessing data from another customer/company by accident or by design?	The separation of data is controlled throughout the application using logical security. Data and documents belong to tests within audits. Users can only access data or documents if they have the necessary permissions for that audit.	Noted - see above
6.10	How is [Internet] communication traffic monitored to identify potential problems before they happen: - From a performance perspective? - From a security standpoint?	<p>AuditBot uses Cloudflare to manage and monitor internet-facing traffic for both its commercial website and application. Cloudflare provides performance optimisation through intelligent caching, content delivery network (CDN) routing, and real-time traffic analytics. This allows us to proactively monitor response times, latency, and traffic anomalies that could indicate performance issues before they impact end users.</p> <p>From a security perspective, Cloudflare offers a robust Web Application Firewall (WAF), DDoS protection, and bot mitigation, helping to detect and block malicious traffic at the edge. Suspicious access patterns, repeated login attempts, and potential exploitation attempts are monitored in real-time and mitigated automatically.</p> <p>In addition to Cloudflare, we use Azure Application Insights to monitor server-side performance and exception handling within the AuditBot platform. This includes tracking unhandled exceptions, slow-running operations, and usage metrics, allowing the development team to detect and address emerging issues promptly.</p>	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?	<p>None</p> <p>While there are no preventive controls in place to reduce the risk of Internet Connection breakage, in the event of a server failure, a server switch can be executed at the backend to maintain continuity.</p>	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?	<p>Yes, all communications between the user's browser and the AuditBot platform are encrypted using TLS (Transport Layer Security). This includes not only login credentials but all data transmitted during the user session — including document uploads, test results, audit metadata, and any interaction with the platform.</p> <p>AuditBot enforces HTTPS across all endpoints, ensuring that data in transit is fully protected against interception, tampering, or eavesdropping. TLS encryption is applied consistently throughout both the commercial website and the core application, supporting compliance with data protection legislation and industry best practices.</p>	Noted
6.13	Is data on your servers encrypted at rest?	Yes	Noted
6.14	What level of encryption is used?	AuditBot uses AES-256 (Advanced Encryption Standard with 256-bit keys) for encrypting data at rest.	Noted
6.15	Is a staging environment provided that is an exact replica of production; which can be used for testing purposes?	Yes but only for development purposes. This is not accessible to end-users.	Noted
6.16	Is a test environment provided to test configuration changes? If so, is there an additional charge for this?	Yes but only for development purposes. This is not accessible to end-users.	Noted



Access to customer data			
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?	<p>AuditBot is hosted on Microsoft Azure within UK-based data centres. Under the UK Data Protection Act 2018 and UK GDPR, customer data remains under the control of the data controller (the audit firm using the platform), while Digital Planning Ltd. acts as the data processor.</p> <p>Although Microsoft (as the hosting provider) physically stores the data, it has no access to the content, as all data is encrypted at rest using AES-256 and governed by strict contractual and technical safeguards. Microsoft Azure is ISO/IEC 27001, 27017, and 27018 certified, and acts as a sub-processor under a standard Data Processing Agreement (DPA) that includes the required data protection clauses.</p> <p>Digital Planning Ltd. mitigates risks by:</p> <ul style="list-style-type: none"> <li>- Hosting all customer data within the UK to avoid international data transfer issues.</li> <li>- Implementing encryption in transit and at rest.</li> <li>- Limiting access to production environments to authorised personnel only.</li> </ul>	Noted
6.18	Are you subject to any legal or regulatory requirements obliging you to retain a copy of	No	Noted
6.19	Who will be able to access or see customer data?	Employees of AuditBot Limited and Digital Planning Limited 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.	<p>AuditBot is hosted on Microsoft Azure, which operates under a zero-trust security model and enforces strict physical and logical access controls within its data centres. Azure staff and contractors do not have access to customer data. Microsoft's infrastructure is governed by a suite of internationally recognised certifications, including ISO/IEC 27001, SOC 2, and ISO/IEC 27018, which includes specific controls to protect against unauthorised internal access.</p> <p>On the vendor side, Digital Planning Ltd. enforces a set of internal procedures to prevent unauthorised access to customer data by staff or contractors:</p> <ul style="list-style-type: none"> <li>- Access Control: Access to production environments is limited to a small group of authorised personnel, and is managed via secure authentication and role-based permissions.</li> <li>- Audit Logging: All access to infrastructure and systems is logged and monitored.</li> <li>- Principle of Least Privilege: Staff are only granted the minimum access required to perform their role, and access is reviewed regularly.</li> <li>- No Default Access: Developers and support staff do not have access to live customer data unless explicitly required for a support case and authorised by senior management.</li> <li>- Confidentiality Agreements: All employees and contractors are bound by confidentiality clauses and security policies aligned with our ISO/IEC 27001 certification.</li> </ul>	Noted

6.21	Explain the release management procedures in place and the associated segregation of duties ?	<p>AuditBot follows formal release management procedures based on Git version control, CI/CD pipelines, and strict segregation of duties:</p> <p>Version Control and Branching: All development work is managed using Git with clearly defined branching strategies (e.g. feature branches, staging, and production branches). This ensures traceability and separation between development, testing, and release stages.</p> <p>CI/CD Pipelines: Code is deployed to production using automated Continuous Integration/Continuous Deployment pipelines. These pipelines include build verification, automated testing, and deployment stages, reducing the risk of human error and ensuring consistent, auditable releases.</p> <p>Segregation of Duties: Developers do not have direct access to the production environment or production data. Only authorised personnel (typically from the DevOps or release management team) can promote code to production via controlled deployment pipelines. This ensures clear separation between those who write code and those who manage its release.</p> <p>No Direct Server Access: Production infrastructure is configured to prevent manual changes. All updates are deployed through automated processes, and infrastructure access is tightly controlled and logged.</p>	Noted
6.22	Is there sufficient segregation of duties preventing system developers from accessing and changing live applications and data files?	Yes, see above.	Noted
6.23	Explain the review and approval procedures covering system operations staff when emergency changes need to be made to live applications and data?	<p>Unscheduled updates to the production environment are handled through a defined hotfix release process, which is reserved for urgent or critical issues that impact system stability, security, or functionality.</p> <p>When an emergency change is required:</p> <ul style="list-style-type: none"> <li>- The issue is first assessed by senior technical staff to confirm its urgency and scope.</li> <li>- A dedicated hotfix branch is created in Git to isolate the change from ongoing development work.</li> <li>- The fix is peer-reviewed and tested in a controlled environment before deployment to production.</li> <li>- Deployment is carried out via our standard CI/CD pipeline, ensuring consistency and traceability.</li> <li>- All emergency changes are retrospectively documented and reviewed by the development and operations team, including justification, risk mitigation steps, and testing outcomes.</li> </ul>	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?	<p>AuditBot and its underlying infrastructure are designed to enforce strict access control procedures, particularly in relation to staff offboarding.</p> <p>Azure Role-Based Access Control (RBAC): Access to production resources — including databases, storage accounts, and services — is managed via Microsoft Azure Resource Groups with RBAC. Developers and operations staff do not store credentials locally; access is granted dynamically and can be revoked immediately upon staff departure.</p> <p>Immediate Revocation: When a staff member leaves, their Azure account is disabled or removed, which automatically revokes access to all application resources, even if they have a local copy of the codebase. This ensures there are no residual credentials or tokens that could be misused.</p> <p>Tooling and Internal Systems: Access to email, source control (e.g. Git repositories), documentation platforms, and support tools is managed centrally and removed systematically as part of our offboarding checklist. The process is overseen by senior management to ensure completeness and traceability.</p> <p>Zero Standing Access Policy: We follow a least-privilege model and do not provide standing access to sensitive systems. All access is provisioned on a need-to-use basis and reviewed regularly.</p>	Noted
<b>Platform and service levels</b>			
6.26	Which databases and servers are used to host the software?	<p>AuditBot is hosted on Microsoft Azure, using a modern cloud-native architecture. The core components include:</p> <p>Web Application: Built with .NET Blazor and deployed via Azure App Services.</p> <p>Database: Hosted on Azure SQL Database, a fully managed relational database service based on Microsoft SQL Server, with built-in high availability, encryption at rest, and automated backups.</p> <p>Document Storage: All uploaded audit documents are stored in Azure Blob Storage, which supports secure and scalable file management.</p>	Noted
6.27	What forms of user authentication are supported e.g. user names, passwords certificates, tokens etc.?	<p>AuditBot currently supports username and password-based authentication for all users. Passwords are securely hashed using PBKDF2 with HMAC-SHA256, in line with best practice under ASP.NET Core Identity. Users are required to create a strong password during account setup, and password reset functionality is provided through secure, time-limited email links.</p> <p>Additional forms of authentication are on our roadmap:</p> <p>Multi-Factor Authentication (MFA) is scheduled for implementation in the FFR, which will add a second verification step (e.g. code via email). See question 3.09.</p> <p>Single Sign-On (SSO) support is also planned (Q1 2026), including integration with enterprise identity providers such as Microsoft Entra ID (formerly Azure AD), using OAuth2 or SAML 2.0 protocols.</p>	<p>Noted</p> <p>See conclusion point 2.08</p>
6.28	What is the proposed product/service availability percentage?	n/a	n/a
6.29	What percentage availability has been achieved over the past 12 months?	n/a	n/a
6.30	Is a service level agreement ("SLA") offered regarding: - Service availability? - Data recovery?	No	Noted

6.31	Is the service available 24x7 or are there downtime periods for maintenance?	Service is available 24/7, with new versions and releases held in development before being pushed live.	Noted
6.32	Is the customer made aware of maintenance periods in advance?	n/a	n/a
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?	No software is required to be installed.	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?	n/a	n/a
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.	No	Noted
<b>Platform security</b>			
6.36	What security steps are taken to prevent and detect intrusion attempts?	Cloudflare is used as a secure edge layer for both the application and website. This provides:  Web Application Firewall (WAF) for blocking common attack patterns (e.g. SQL injection, XSS)  DDoS mitigation and rate limiting  Bot filtering and IP reputation monitoring	Noted
6.37	Is firewall hardware and software used to protect the live systems from unauthorised access?	AuditBot is hosted on Microsoft Azure, which provides built-in intrusion detection, security baselines, and enterprise-grade monitoring.  All infrastructure is protected by Azure Security Centre, which actively scans for vulnerabilities and applies recommended hardening measures.	Noted
6.38	Which monitoring software is used to create alerts when intrusion attempts are suspected?	Azure Security Control	Noted
6.39	Are designated staff responsible for receiving and urgently responding to these alerts?	Yes	Noted
6.40	Have clear procedures been established for identifying and responding to security incidents?	Members of the development team participate in a duty rota to be available to respond to security incidents.	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, this is provided as part of the managed hosting service by Azure.	Noted
6.42	List the procedures and software tools in place to prevent or detect and eliminate interference from malicious code, such as viruses?	We use Vanta to continuously scan the code repository for malicious code signatures and vulnerable code.	Noted

6.43	<p>Is a system log maintained by the service provider that details</p> <ul style="list-style-type: none"> <li>- User access?</li> <li>- User activity?</li> <li>- Error messages?</li> <li>- Security violations?</li> </ul>	<p>Yes, system logging is in place across multiple levels of the AuditBot platform, using a combination of Azure Application Insights and internal logging mechanisms. These logs support monitoring, diagnostics, and ongoing system improvement:</p> <p>User Access: Logs are maintained for successful logins and failed login attempts. These include timestamps, user IDs, and IP addresses, enabling basic access auditing and threat detection.</p> <p>User Activity: While a formal, user-facing audit trail is under development, user interactions with key system functions (e.g. test executions, document uploads, and API calls) are logged internally. This information can be used for diagnostic and security review purposes.</p> <p>Error Messages: All application-level errors, including unhandled exceptions and failed service calls, are captured in Azure Application Insights, with full context for debugging and resolution. This supports real-time alerting and proactive issue resolution.</p> <p>Security Violations: Suspicious activity such as repeated failed login attempts or malformed requests is tracked via Cloudflare's security analytics and Azure Security Centre, allowing for early identification of potential intrusion attempts.</p>	Noted
6.44	Is this log available to the customer?	No	Noted
6.45	<p>Have there been any successful unauthorised access attempts been made during the last year?</p> <p>If Yes:-</p> <ul style="list-style-type: none"> <li>- What was the effect on the business and users?</li> <li>- What steps are in place to prevent this happening again?</li> </ul>	<p>No</p> <p>System is not live therefore this has not been tested.</p>	Noted - system is not live.
6.46	<p>Is penetration testing regularly carried out by (please indicate frequency of tests):</p> <ul style="list-style-type: none"> <li>- Staff specialising in this field?</li> <li>- External specialists?</li> </ul>	Yes. Qualys (penetration testing) and Vanta (vulnerability scanning) are used for continuous automated security testing.	Noted
6.47	Are procedures in place to ensure that any weaknesses found by penetration testing are addressed quickly?	Yes, but only for development purposes. This is not accessible to end-users.	Noted
6.48	If penetration testing by a specialist is not performed regularly, please indicate the main procedures in place to identify weaknesses?	n/a	n/a
6.49	<p>Are security procedures regularly reviewed?</p> <p>Please indicate frequency of reviews.</p>	Yes quarterly.	Noted
6.50	What security reporting is provided demonstrating compliance against certification(s) and policy(ies)?	Vanta helps organizations demonstrate security and compliance through its trust management platform, offering tools like Trust Reports and Trust Centres for showcasing compliance data and streamlining security reviews, as well as automated compliance solutions for frameworks like SOC 2, ISO 27001, and GDPR. For example, Azure compliance details are available here: <a href="https://learn.microsoft.com/en-gb/azure/compliance/">https://learn.microsoft.com/en-gb/azure/compliance/</a>	Noted
6.51	How are security breaches communicated to customers?	Via email mailing list, and in serious cases telephone.	Noted

Backups by the service provider			
6.52	<p>In relation to backups undertaken by the system provider please explain:</p> <ul style="list-style-type: none"> <li>- How is a customer's data backed up?</li> <li>- How often is this undertaken?</li> <li>- What is backed up?</li> <li>- What's the media used?</li> <li>- Where are backups stored?</li> <li>- How many copies are there?</li> <li>- How long are they retained for?</li> <li>- Who has access to them?</li> <li>- Is the data encrypted?</li> </ul>	<p>AuditBot's customer data is hosted on Microsoft Azure, and all backups are managed in accordance with Azure's enterprise-grade backup and recovery services. Our backup procedures ensure business continuity and compliance with relevant data protection and professional standards:</p> <p>1. How is a customer's data backed up? Backups are performed using Azure Backup and Azure SQL automated backups, which create point-in-time snapshots of both structured data (Azure SQL Database) and unstructured data (document uploads stored in Azure Blob Storage).</p> <p>2. How often is this undertaken? Database backups occur multiple times per day (transaction-level backups), with full backups typically taken daily.</p> <p>Blob storage (uploaded files) is protected through redundant replication and versioning to guard against deletion or corruption.</p> <p>3. What is backed up? Customer audit data stored in the Azure SQL Database (test data, user accounts, metadata)</p> <p>All uploaded documents and working papers stored in Azure Blob Storage</p>	Noted
6.52 cont.		<p>4. What's the media used? Backups are stored digitally within the Azure cloud environment, using Azure's managed and secure storage services — no physical media is involved.</p> <p>5. Where are backups stored? All backups are stored within Microsoft Azure data centres located in the UK South region, ensuring compliance with UK data residency requirements.</p> <p>6. How many copies are there? Backups are maintained using locally redundant storage (LRS) options, ensuring multiple encrypted copies exist across separate physical locations.</p> <p>7. How long are they retained for? Database backups are retained for up to 35 days. Document storage incorporates soft-delete and versioning, allowing recovery of deleted or overwritten files within a configurable retention window.</p> <p>8. Who has access to them? Access to backups is strictly limited to authorised DevOps personnel within Digital Planning Ltd. Access is controlled via Azure role-based access control (RBAC) and all actions are logged and monitored.</p>	
6.52 cont.		<p>9. Is the data encrypted? Yes. All backup data is encrypted at rest using AES-256 and in transit using TLS 1.2 or higher, in alignment with Azure security standards and the requirements of ISO/IEC 27001 and UK GDPR.</p>	
6.53	How frequently is a test-restore of backups undertaken?	Quarterly	Noted
6.54	Can the provider restore from a backups that it has taken at a customer request?	Not currently.	Noted
6.55	Does a customer have the ability to undertake their own backups?	No	Noted - this is not unusual for a SaaS product
6.56	If so, can a customer restore data a backup that they have taken?	n/a	n/a

Platform recovery			
6.57	<p>What contingency plans are in place to enable a quick recovery from:</p> <ul style="list-style-type: none"> <li>- Database or application software corruption?</li> <li>- Hardware failure or theft?</li> <li>- Fire, flood and other disasters?</li> <li>- Communication failures?</li> </ul>	<p>AuditBot is hosted on Microsoft Azure, which provides a resilient and secure infrastructure with built-in capabilities to support rapid recovery in the event of failure or disaster. Our contingency planning covers the following key areas:</p> <p>1. Database or Application Software Corruption Point-in-time backups of the Azure SQL Database are taken regularly, allowing data to be restored to any point within a 35-day retention window.</p> <p>Application deployments are managed through CI/CD pipelines with version control, enabling quick rollback to a previous stable release if software corruption is detected.</p> <p>All deployments are tested in staging environments prior to production release to minimise the risk of faulty code reaching live systems.</p> <p>2. Hardware Failure or Theft Microsoft Azure provides full hardware redundancy and automated failover as part of its managed services. In the event of hardware failure, services are automatically redirected to healthy nodes with no data loss.</p> <p>As AuditBot runs entirely on Azure infrastructure, no data is stored on local hardware at Digital Planning, mitigating the risk associated with device theft.</p>	Noted
		<p>3. Fire, Flood, and Other Disasters Azure data centres are tier 4 facilities designed to withstand major environmental events. Azure maintains disaster recovery protocols, including geographically distributed data replication and site-level failover capabilities.</p> <p>AuditBot's use of geo-redundant storage (GRS) ensures data is replicated across multiple physically separated facilities within the UK region.</p> <p>4. Communication Failures Azure's globally distributed Content Delivery Network (CDN) and Cloudflare edge services help mitigate the impact of regional connectivity issues.</p> <p>Uptime and response times are actively monitored, and 24/7 escalation procedures are in place to investigate connectivity issues quickly.</p> <p>Failures in client-side connectivity do not impact data integrity, as no partial transactions are written without full validation and confirmation.</p> <p>Recovery Objectives The platform is designed to support a Recovery Time Objective (RTO) of under 4 hours and a Recovery Point Objective (RPO) of under 15 minutes for database operations.</p>	
6.58	How often are these plans tested?	Quarterly	Noted
6.59	How often are these plans reviewed and updated?	Quarterly	Noted
6.60	What is the longest period of time envisaged that service may not be available?	1 hour	Noted

6.61	What are your: - Recovery Point Object (RPO) standards? - Recovery Time Objective (RTO) minimum standards?	AuditBot operates with the following recovery objectives:  Recovery Point Objective (RPO): Less than 15 minutes Azure SQL Database uses frequent transaction log backups, allowing the database to be restored to a point in time within the most recent 5–15 minutes in the event of data loss or corruption.  Recovery Time Objective (RTO): Less than 4 hours The platform is designed to be restored from backup and redeployed using automated CI/CD pipelines, enabling full platform recovery — including application services and data — within 4 hours under normal recovery conditions.	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?	All dates and times are presented using London time (EN GB locale)	Noted
6.63	What protection is in place to enable users to be 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?	AuditBot is a supplementary tool and all data is exported during testing. On this basis AuditBot is not a source of truth and should not be relied on as such.	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?	n/a	n/a
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?	n/a	n/a
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
<b>Platform change management</b>			
6.67	Describe your approach to upgrades including what option customers have not to take upgrades (if any)?	AuditBot is a SaaS platform and therefore updates are mandatory, users cannot opt out.	Noted
6.68	Are users able to test the application before new versions go into live use?	User Acceptance Testing (UAT) will occur with trusted clients for any large future releases as and when required. There will be no general access to upcoming versions in the near future.	Noted
6.69	Are users given notice before application changes are applied to the live system?	The release schedule will be established at launch and users will be notified of upcoming and past releases via the website.	Noted
6.70	Are changes delivered into the live environment "switched off" to enable users to test them before enabling them for their environment?	Updates will not be pushed to production without unit and QA testing, in accordance with the sprint approach	Noted
6.71	Describe what testing and QA processes are undertaken before upgrades and other changes are made live/available to customers?	We have a dedicated QA team with audit experience. The QA testing team works through each development task within each sprint. Nothing is pushed to production without the oversight of the QA testers.	Noted
6.72	Explain the release management procedures in place and the associated segregation of duties?	All features are tested during development. Each release candidate is tested in full prior to release scheduling. A final testing checklist is completed on the production environment after each new release.	Noted
6.73	Are users informed when they next login of the application changes that have gone into live use?	We have on our roadmap a feature to display a news summary to users on the initial dashboard screen after logging in. This news summary will include new releases and link to the changelog. This feature is planned for Q4 2025.	Noted See conclusion point 2.08



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.	No - however extended QA processes are being performed which includes UAT on a staging server.	Noted - note that full regression testing is recommended to test system under a code freeze environment pre FFR.  See conclusion point 2.09
<b>Subscription options</b>			
6.75	What is the minimum level of commitment must the customer sign up to, e.g. 36 months?	None as standard. Agreements are made on a case by case basis.	Noted
6.76	Where online payment is used, what type of security is used to protect sensitive information?	AuditBot uses Stripe Checkout Elements, a fully hosted and PCI-compliant payment solution, to manage online payments. As a result, no cardholder data is captured, processed, or stored by AuditBot or Digital Planning Ltd. directly.  All sensitive payment information — such as credit card numbers and billing details — is entered on Stripe’s secure, off-site platform, which is certified to PCI DSS Level 1, the highest level of payment security compliance. The integration uses TLS encryption to ensure all payment data is securely transmitted between the user's browser and Stripe’s servers.  Billing and subscription management are handled manually via the Stripe dashboard, further reducing exposure to sensitive financial data and ensuring full alignment with data protection and security standards.	Noted
6.77	Where online subscription / payment is used, is an invoice provided to the customer and, if so, in what format?	Yes. Digital format, monthly in arrears.	Noted
6.78	When subscriptions need to be renewed, what advance notice is provided and what is the time limit for renewal?	n/a	n/a
6.79	Is there a procedure for late renewal and is there a time limit after which subscriptions cannot be renewed?	n/a	n/a
6.80	How soon after creating or renewing a subscription (if applicable) can the system / service be used?	n/a	n/a
6.81	What notifications / confirmations are provided to the customer regarding subscriptions and payments?	AuditBot does not use subscriptions or recurring payments. Instead a payment method must be attached to each Audit Firm and payments are billed in arrears at the end of each month based on usage. Payments are raised against the stored payment method and the card holder must approve each payment via their banking platform.	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?	n/a	n/a
6.83	At the end of the contract term, how long does a customer have to obtain a copy of their data from you?	AuditBot data persists indefinitely in the application. So that users can login anytime in the future to access it. This policy may change as our storage requirements increase.	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?	AuditBot is billed based on usage so there are not contract terms. Data is anonymised automatically after 2 years. This feature is planned for release in Q4 2025.	Noted  See conclusion point 2.08
6.85	What is your process regarding disposal of end-of-life and failed hardware devices that were used to operate your service?	n/a	n/a
<b>SaaS/Hosted Reporting</b>			
6.86	Are reports produced from the same software as the financial applications or is separate reporting software used?	n/a	n/a
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	Noted
6.88	What browser versions are support: - On desktop/laptop (PC, Mac, Linux)? - On Tablets? - On mobiles?	Google Chrome and Microsoft Edge are supported currently on desktop/laptop. There aren't currently mobile or tablet versions of AuditBot.	Noted

6.89	Is access to the reporting facilities and data controlled by the same procedures as access to the main application?	Yes	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?	n/a	n/a
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?	XSLX and web-based reports	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?	Reports are stored on the user's computer. They are downloaded from the server but they are generated on request, so a file copy of the reports do not exist on the web server.	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?	No	Noted
6.94	Are communications between the browser and the server encrypted for any report related communications?	All communication is encrypted using TLS HTTPS	Noted
6.95	If reports are produced dynamically each time the user views them can historical reports be reproduced at any time?	No	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?	No	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?	n/a	n/a
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?	Exports are made in XSLX format. This is a binary format that cannot be opened if the file is not complete.	Noted

Ref	Requirement	Response	Reviewer Comments
7.00	<b>Audit testing software</b>	NB: "audit firm" used to refer to customers of AuditBot, whereas "audit client" refers to clients of the audit firm of which the firm is	
<b>Functionality</b>			
7.01	How does a user create an account?	<p>The super user of an AuditBot audit firm account would typically be a partner of an audit firm. The 'super user' will therefore will be the single point of contact for the audit firm.</p> <p>Steps include:</p> <p>(1) Personal Information - AuditBot requests the following information:</p> <ul style="list-style-type: none"> <li>- Name</li> <li>- Email</li> <li>- Phone Number</li> </ul> <p>(2) Verify email address - 6 digit code to verify email.</p> <p>(3) Create password - requests two password entries.</p> <p>(4) Company information - AuditBot requests the following business information of the audit firm:</p> <ul style="list-style-type: none"> <li>- Company Name</li> <li>- Street Address, City, Postcode, Country</li> </ul>	<p>Confirmed</p> <p>(3) Password Security: Not sighted as at 14 April 2025 however understand that - The Microsoft Identity Framework integration will be in the FFR and will include requirements for passwords minimum length and complexity criteria. Including password history policy.</p> <p>See conclusion point 2.07</p>
7.02	Is payment managed through the tool?	<p>High level payment process includes:</p> <p>(1) Pay as you go process - no enterprise agreements currently however are looking to implement this in the future.</p> <p>(2) Payment process will form part of the 'create account' process.</p> <p>(3) AuditBot will request credit card information - this will be pre charged monthly.</p> <p>Using Stripe for payment integration.</p> <p>(4) Billing will be done in accordance with the audit firm's agreement with AuditBot.</p>	<p>Noted - payment process was not sighted as at 14 April 2025, however understand that it is planned for FFR.</p> <p>See conclusion point 2.07</p>
7.03	How to invite other people to an Audit team?	<p>The 'super user' has the ability to add and amend user access for their colleagues supporting on audit testing.</p> <p>*Currently there is one super user per audit firm. However there are plans to expand this as the solution grows.</p>	Noted
7.04	How are individual audit files created for audit clients?	The super user can create new client accounts by inserting the client name and registered company number.	Confirmed
7.05	How to create a new audit?	<p>The super user can create new audits through the following steps:</p> <p>(1) The Client must already be created in the AuditBot system to create an audit</p> <p>(2) Once client has been selected, add audit end date using a dd/mm/yyyy field and confirm audit start date (dd/mm/yyyy field) which AuditBot estimates is 365 days prior to the end date (although this can be manually modified).</p> <p>(3) Upload nominal code template for that client. Requests a CSV file. Max size is 20MB</p> <p>(4) Upload nominal ledger for that client. Requests an xlsx file. Max size 50MB</p> <p>(5) Further files can then be uploaded at this stage, as well as adding further team members</p> <p>(6) Audit is then completed and relevant tests can be selected to proceed with testing and allocate to team members</p>	Confirmed

7.06	What tests are available for clients using the tool?	<p>First Functional Release:</p> <p>For the FFR AuditBot are only releasing tests that are related to the P&amp;L, this will include purchasing, sales and wages.</p> <p>As at 14 April 2025 Live tests include:</p> <p>Sales - Walkthrough Test - Goods</p> <p>Sales - Walkthrough Test - Services</p> <p>Sales - Transaction Test Completeness Services</p> <p>Sales - Transaction Occurrence</p> <p>Sales - CutoffTest - Goods</p> <p>Sales - Cutoff Test - Services</p> <p>Sales - Transaction Test Completeness Goods</p> <p>Purchase - Walkthrough Test - Goods</p> <p>Purchase - Walkthrough Test - Services</p> <p>Purchase - Transaction Test</p> <p>Purchase - Cutoff Test - Goods</p> <p>Purchase - Cutoff Test - Services</p> <p>Wages - Walkthrough Test</p> <p>Wages - Transaction Test</p> <p>Wages Reconciliation Test - Monthly</p> <p>Wages Reconciliation Test - Weekly</p> <p>*AuditBot is a solution for a sub-set of fieldwork (an assistive tool to help existing workflows) it is not an end to end audit solution, therefore it is not in a position currently to define all tests required for an audit file.</p>	<p>Confirmed - FFR functionality sighted 14 April 2025.</p> <p>However an end to end demonstration was only performed for one of these tests, the Sales - Transaction Test Completeness Services.</p> <p>An offline demonstration of the Wages Reconciliation Test - Monthly test was also retrospectively shared.</p>
7.06 cont.		<p>Future Releases:</p> <p>Balance sheet functionality, bespoke testing and non financial tests are planned for future releases.</p>	
7.07	What is involved to set up an audit test?	<p>As at 14 April 2025 - Demo included:</p> <p>Sales - Transaction Test Completeness Services</p> <p>This test included:</p> <p>(1) Uploading Nominal Ledger (the unique identifiers for the data, e.g., Order Reference number) - this helps with the matching functionality.</p> <p>(2) Details of the Sample. This requests:</p> <ul style="list-style-type: none"> <li>- Audit area (e.g., sales)</li> <li>- Assertions</li> <li>- Definition and expectation of error</li> <li>- Source of test sample</li> <li>- Stratification</li> <li>- Total population value (£)</li> <li>- Sample size (manual)</li> </ul> <p>(3) Software then requests files relevant to the audit (sales orders and invoices) for the required sample.</p>	<p>Confirmed - demonstration of the Sales - Transaction Test Completeness Services was performed on 14 April 2025.</p> <p>An offline demonstration of the Wages Reconciliation Test - Monthly test was also retrospectively shared.</p> <p>See conclusion point 2.05</p>

7.08	What is the core functionality ?	<p>Within a test AuditBot performs matching functionality.</p> <p>As at 14 April 2025 - Demo included: Sales - Transaction Test Completeness Services:</p> <p>(1) Once the audit is set up, the auditor is required to upload evidence for the test. In the example of the Sales - Transaction Test Completeness Services, this included sales orders and sales invoices. (For wages reconciliation, this includes payroll report and trial balance.)</p> <p>(2) AuditBot then reviews this data, using OCR technology.</p> <p>(3) Once the analysis is complete, AuditBot presents a display of the information scanned and the data is has extracted (e.g., sales: order data, invoice total, order reference, sub total, vendor name, wages: pensions, NI, salaries). This allows the user to verify the information has been accurately extracted and amend any errors if required.</p> <p>(4) AuditBot then presents the matched data in a display. In the event there are conflicts / samples that do not match, this is presented with a red pop up box at the top of the screen, and the sample number is also highlighted in red to present the error. Any errors require a manual approval or rejection. In the case of the wages testing, the balance from both sources is shown, with the difference highlighted with a dropdown box to highlight whether this is material.</p>	<p>Confirmed - demonstration of the Sales - Transaction Test Completeness Services was performed on 14 April 2025.</p> <p>An offline demonstration of the Wages Reconciliation Test - Monthly test was also retrospectively shared.</p> <p>See conclusion point 2.05</p>
7.09	How are results displayed?	<p>Once test is complete results can be exported into excel. For the demo on 14 April 2025 for the Sales - Transaction Test Completeness Services Setup. This involved:</p> <p>(1) Test Tab outlining:</p> <ul style="list-style-type: none"> <li>- Objective</li> <li>- Sample size</li> <li>- Method</li> <li>- Results</li> <li>- Mis-statements</li> <li>- Conclusion</li> </ul> <p>(2) Results Tab</p> <p>Excel table with key matching test data for that particular test.</p>	<p>Confirmed - demonstration of the Sales - Transaction Test Completeness Services was performed on 14 April 2025.</p> <p>An offline demonstration of the Wages Reconciliation Test - Monthly test was also retrospectively shared.</p> <p>See conclusion point 2.05</p>
7.10	Are multiple currencies supported?	Yes - FX rates can be defined on the results screen of the audit test.	Confirmed
7.11	Is materiality considered? If so, where within the software?	Materiality figures are entered by the auditor during tests where it is relevant. The auditor is required to mark test results as trivial, non-trivial or material in tests where it is appropriate.	Noted
7.12	How does the software ensure readability accuracy?	Confidence scores are provided for each field that is read by Azure Cognitive Services (Part of Azure Document Intelligence service). Confidence scores are calculated based on AI training data comprising of millions of documents.	Noted

7.13	What functionality is on the roadmap for future releases?	<p>AuditBot High-Level Roadmap</p> <p>For launch: Login security (MFA, Password Strength, Password History, session timeout) Q2 2025</p> <p>2025:</p> <p>In-app activity log report (audit trail) Q3 2025 (see Q 3.21, 4.14 &amp; 4.21)</p> <p>Detailed system logging Q3 2025 (see Q 3.22)</p> <p>API link to client accounting systems Q3 2025 (see Q 7.15)</p> <p>Combine bank statements Q3 2025</p> <p>MFA using Authenticator app Q4 2025</p> <p>In-app notifications Q4 2025 (see Q 5.11)</p> <p>Dashboard news widget including upcoming release announcements + changelog Q4 2025 (see Q 6.73)</p> <p>Balance Sheet tests Q4 2025</p> <p>Custom testing Q4 2025</p> <p>2026:</p> <p>End-to-end inspection of audit transactions Q1 2026 (see Q 4.29)</p> <p>Single Sign On (SSO) Q1 2026 (see Q 3.01, 3.08, 3.10 &amp; 6.27)</p> <p>Client Portal Q1 2026 (see Q 3.05 &amp; 7.16)</p>	<p>Noted</p> <p>See conclusion point 2.08</p>
7.14	Is it possible for users to create bespoke tests ?	It is not possible to create bespoke tests currently in AuditBot. This is on our roadmap but does not have a scheduled date at this time.	Noted
7.15	What integrations does the tool support?	<p>The platform supports importing account codes from IRIS accounting software, with integrations for CaseWare and CCH scheduled for release later this year. We are also implementing a connection to Merge.dev, which will allow integration with a wide range of online accounting platforms and this is due to be released in Q3 2025.</p> <p>Imported account codes are validated for uniqueness and structure during the import process.</p>	<p>Noted</p> <p>See conclusion point 2.08</p>
7.16	Does the tool support audit client access?	Client access is not in scope for FFR however is planned for the second or third release. This will enable clients to directly upload test data, nominal codes and nominal ledgers. This feature is planned for release in Q1 2026.	<p>Noted</p> <p>See conclusion point 2.08</p>