Ref	Requirement		
	HEADER		
	ICAEW Technical Accreditation Scheme **Digital Bank Analysis Software Evaluation**		
	Altia		
	Jul-26		
	© 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		
	-- *SPECIFIC REQUIREMENTS:*		
7	Digital Bank Statement Analysis		

Ref	Requirement	Response	Reviewer Comments
1	**INTRODUCTION AND PROLOGUE**		
Introduction			
1.01	The suitability of software for each particular user will always be dependent upon that user's individual requirements. These requirements should therefore always be fully considered before software is acquired. The quality of the software developers or suppliers should also be considered at the onset.		
1.02	Fundamentally, good software should: 1. Be capable of supporting the functions for which it was designed. 2. Provide facilities to ensure the completeness, accuracy, confidentiality and continued integrity of these functions. 3. Be effectively supported and maintained. It is also desirable that good software should: 4. Be easy to learn, understand and operate. 5. Make best practical use of available resources. 6. Accommodate limited changes to reflect specific user requirements. It is essential, when software is implemented, for appropriate support and training to be available.		
Approach to evaluation			
1.03	The objective is to evaluate a product against a set of criteria developed by the ICAEW to ensure that the software meets the requirements of Good Accounting Software, as laid down in the summary.		
1.04	In order to effectively evaluate the software, a product specialist from the vendor completed the detailed questionnaire and provided it to the ICAEW to examine. The ICAEW's Scheme Technical Manager then reviewed the operation of the various aspects of the software assisted by a member of the vendor's technical staff and checked the answers to confirm their validity. The questions were individually reviewed and commented on and the majority of assessments were confirmed.		
1.05	The Technical Manager discussed the assessment with a member of the vendor's staff in order to clarify any points requiring further information. In the event of disagreement between the supplier and the Technical Manager, the Technical Manager's decision was taken as final and the response was changed accordingly.		
1.06	The latest version of the software was used throughout the evaluation.		
1.07	When the evaluation had been completed, a draft copy was sent to the ICAEW Scheme Manager for review before completion of the final report.		

Prologue: Matters to consider before purchase		NB: This text has been provided directly by the software vendor and does not form part of the ICAEW's & RSM's evaluation	
1.08	General Overview:	Altia Financial Investigator is a secure, cloud delivered investigative platform designed to support financial investigations, fraud detection, and evidential analysis. It combines Altia’s market leading Financial Investigation Toolkit with a managed Windows 365 Cloud PC environment, enabling investigators to securely ingest, analyse, visualise, and report on large and complex financial datasets while meeting UK public sector security requirements.	
1.09	Supplier background:	Altia Solutions Limited is a long established UK software provider specialising in intelligence led investigation solutions. Altia has developed its Financial Investigation Toolkit in partnership with financial investigators and fraud practitioners and confirms it is used by all UK police forces, multiple government departments, local authorities, and private sector organisations. The toolkit has been described as a market leading bank statement conversion and analysis tool with over twenty years of operational use.	
1.10	Product background and suitability for the user:	Altia Financial Investigator is designed specifically for investigators who need to convert, analyse, and interpret large volumes of financial data for operational and evidential purposes. The platform supports: - OCR based re digitisation of paper and electronic financial records - Merging and analysis of multiple datasets - Pattern, trend, and anomaly detection - Production of evidential reports suitable for court use The solution is suitable for police, regulatory, and government users requiring repeatable, defensible, and efficient financial analysis within a controlled and auditable environment.	
1.11	Add-on modules:	Altia Financial Investigator includes access to a broad set of analytical and productivity tools within the Financial Investigation Toolkit, including: Pattern Manager Merge Accounts Append Worksheets Transaction Matcher Inflation Calculator (CPIH based) Transaction Attachments (file, note, scan, and cheque image linking) Power BI Add In (available for cloud hosted Financial Investigator users) These modules extend core functionality without requiring third party tools and are designed to support end to end investigative workflows.	

1.12	Typical implementation [size]:	Altia Financial Investigator can be implemented for individual investigators, teams, or enterprise scale deployments. Licensing supports both workstation and concurrent usage models, enabling organisations to scale access across departments while controlling costs. Cloud hosted environments are provisioned following receipt of a purchase order, with cloud licence server configuration typically completed within a short operational timeframe.	
1.13	Vertical applications:	The solution is primarily deployed within: - Law enforcement - Government investigative and regulatory bodies - Fraud and financial crime investigation units - Public sector compliance and assurance teams - Insolvency and restructuring firms - Private sector accountancy firms Its functionality is aligned to financial investigation, asset recovery, fraud detection, and evidential preparation use cases.	
1.14	Server platform and database:	Altia Financial Investigator is hosted on Microsoft Azure, using Windows 11 Cloud PCs to provide users with a dedicated, secure Windows environment. This enables access to Microsoft Excel and the Financial Investigation Toolkit within an Altia managed Microsoft tenant dedicated to the customer. Data processed within the toolkit remains within the customer's controlled environment, supporting public sector security and compliance expectations.	
1.15	Client specification required:	For cloud hosted deployments, client requirements are minimal and primarily relate to secure network access and user authentication. For on premise deployments, supported environments include Windows 8.1 or later, Windows 10, Office 2013 and above, and 64 bit operating systems. Use within thin client or Citrix environments requires prior agreement due to third party licensing constraints.	
1.16	Partner network:	Altia is the manufacturer and has a vast third party partner reseller network for Altia Financial Investigator. Delivery, support, licensing, and ongoing product development are provided directly by Altia's internal Product, Customer Success, Training, and Support teams.	

Ref	Requirement		
2.	ISSUES AND CONCLUSION		
Highlighted issues			
2.01	**There are a number of limitations in the product, which while not adversely impacting upon this evaluation may be of importance to some organisations. It is important that any business contemplating the purchase of software reviews the functionality described and limitations therein against its detailed requirements. Attention is drawn in particular to the following areas where the product, on its own, may not be suitable for businesses with certain requirements:**		
2.02	Findings for considerations by potential customers: (See vendor comments against the various questions)	**Question reference**	
*	The system does not currently support role-based access controls, meaning all users operate with the same level of permissions. Where segregation of duties is a requirement, this may increase the risk of unauthorised changes, as access cannot be restricted by role. This risk is partly mitigated by supplementary access controls outside of the application, including controlled access to the Windows Cloud PC / local workstation, customer-managed user authentication, licence based access enforcement, and secure cloud licence validation. These controls restrict who can access the environment, although they do not provide role-based restrictions in the application itself.	3.02-3.06, 7.16-7.19	
*	The system does not integrate with bank feeds or Open Banking APIs, requiring manual data ingestion. As a result, transactions may be edited or deleted during or after import, and the solution does not maintain a system generated audit trail of user actions (e.g. edits, deletions, imports). This limits traceability and reduces the ability to evidence data integrity from source data through to analysis. The impact is partly mitigated by the product's import validation and transaction checking functionality, including balance checks, duplicate/linked transaction detection, and error highlighting. However, these validation controls do not replace a system-generated audit trail and do not prevent users from manually amending data during analysis. Where such end to end traceability is required, this represents a significant control gap and may restrict suitability in regulated environments. While this may be less critical where the tool is used purely for analytical purposes, there remains an increased risk of incomplete or altered datasets.	3.17–3.24, 7.04–7.06, 7.12, 7.47–7.48	
*	The solution relies heavily on Excel for data storage and processing, introducing risks around version control, manual errors, and lack of embedded system controls.	3.29, 4.20, 5.04, 5.05	
*	The lack of file locking or multi-user controls increases the risk of data overwrites and inconsistencies when multiple users access the same files.	5.04, 5.05	
*	The absence of a standardised risk scoring model means users must manually define rules, reducing consistency and repeatability of analysis.	7.15, 7.73	

Evaluation conclusion			
2.03	For the specific use-cases in support of assisting accountancy firms to make effective use of Digital Bank Analysis software, for which the product is designed, the solution appears to meet this criteria. It continues to be actively developed and enhanced. Members should be aware of the limitations of the solution as above, and fully understand the role that it can play in helping manage their compliance needs. * NOTE THAT THE QUESTIONNAIRE RELATES TO THE SOFTWARE PRODUCT AND NOT ANY SUPPLEMENTARY SERVICES PROVIDED BY THE SUPPLIER TO THE ACCOUNTANCY FIRM USING THAT PRODUCT *		
Disclaimers			
2.04	Any organisation considering the purchase of this software should consider their requirements in the light of proposals from the software supplier or its dealers and potential suppliers of other similarly specified products. Whilst the contents of this document are presented in good faith, neither ICAEW, nor the ICAEW's Technical Manager (RSM UK Consulting LLP or any party nominated by the ICAEW to perform this role on the ICAEW's behalf) will accept liability for actions taken as a result of comments made herein. The decision to purchase software resides entirely with the organisation.		

Ref	Requirement	Response	Reviewer comments
3.	**ACCESS AND SECURITY**		
Access control			
3.01	What security features are included to control access to the application?	Security Features Used to Control Access to the Application Altia Financial Investigator incorporates multiple layered security controls to manage and restrict access to the application and associated data environments: 1. Controlled Cloud Access via Dedicated Environments For cloud hosted deployments, users access the application through a dedicated Windows 365 Cloud PC hosted within Microsoft Azure, provisioned within an Altia managed Microsoft tenant dedicated to the customer. This ensures access is limited to authorised users within a controlled and isolated environment. 2. User Authentication and Environment Access Controls Access to the Financial Investigation Toolkit is governed by: User specific authentication to the Windows Cloud PC or local workstation Customer controlled user account management This ensures that only approved users can access the investigative environment and associated tooling.	Noted, see question 7.80.
3.01 cont.		3. Licence Based Access Enforcement Application access is further controlled through Altia's licensing mechanisms: - Workstation licences, restricting use to named machines - Concurrent licences, limiting the number of simultaneous users Licence enforcement ensures that only authorised, licensed users can operate the software at any given time. 4. Secure Cloud Licence Server Where concurrent licensing is used, access is validated through Altia's Cloud Licence Server, which operates over secure HTTPS connections. Only minimal machine identifier and licence state information is exchanged, with no investigative or customer data stored on the licence server .	
3.01 cont.		5. Secure Development and Governance Framework Altia operates under ISO 27001 and Cyber Essentials Plus, embedding access control into its Security Development Lifecycle. This includes defined security requirements, threat modelling, penetration testing, and incident response planning, ensuring access controls are designed, tested, and maintained in line with recognised UK government security standards .	

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?	Function level access cannot be managed via a granular permissions matrix that hides or exposes specific menus or features per user role. What is supported, and what is not, is outlined clearly below: What is supported Access control is enforced at the environment and licence level, meaning only authorised and licensed users can access the application at all. Users must authenticate to the Windows Cloud PC or local workstation, and must hold a valid workstation or concurrent licence to launch and use the software. Where concurrent licensing is used, simultaneous access is technically restricted via the Altia licence server, preventing unauthorised or excess usage. These controls ensure that only approved users can access the application, but they do not differentiate functionality within the application itself.	Noted.
3.03 cont.		What is not supported The documentation does not describe any role based or permissions matrix capability that would: - Restrict access to specific functions or tools by user role - Hide or show menu options based on authorisation level - Apply fine grained feature level permissions within the application UI All authorised users with access to the Financial Investigation Toolkit have visibility of, and access to, the full set of application features provided under their licence model .	
3.03	Is this access to the application managed by:- - Individual user profiles? - User groups or job roles?	There are two parts to the application a scanning and OCR tool, and an Excel Add In. Users either have the application (and licence) or not. Within that functionality is not targeted at different roles.	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?	The solution provides clear and auditable oversight of user access at the application and environment level, supporting strong governance and security assurance. Access to the Financial Investigation Toolkit is managed through named user provisioning and licence entitlement, ensuring that only authorised individuals are able to access the system. Organisations can readily identify which users have been granted access to the application environment and which users hold valid workstation or concurrent licences, providing a reliable and auditable view of current authorised users. For cloud hosted deployments, user access to the dedicated Windows Cloud PC environment is managed through standard Microsoft account controls, allowing organisations to maintain visibility of provisioned users and enforce joiner, mover, and leaver processes in line with internal security policies.	Noted.
3.04 cont.		The application operates with a consistent functional access model for all authorised users. This simplifies access management, reduces the risk of mis configuration, and ensures investigators have immediate access to the full set of analytical capabilities required to perform their role effectively. As a result, there is no dependency on complex role hierarchies or permissions matrices to maintain system integrity. While the solution does not apply differentiated function level permissions within the application, this approach supports clarity, operational efficiency, and ease of audit, with access control focused on who can access the system rather than restricting investigative capability once access is granted.	
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?	The solution operates with a clear and consistent user interface for all authorised users. Once access to the application has been granted, users are presented with the full set of menu options and analytical tools available within the Financial Investigation Toolkit. This approach delivers several operational and assurance benefits: Clarity and usability – all authorised users have a consistent view of the application, reducing training overhead and avoiding confusion caused by role specific or dynamically changing menus. Reduced risk of mis configuration – the absence of complex, role based menu rules removes the risk of incorrectly applied permissions impacting investigative work. Operational effectiveness – investigators are not constrained by hidden functionality and can immediately access the full analytical capability of the toolset when required.	Confirmed.

3.05 cont.		Menu display is therefore not dynamically restricted based on user specific permissions, as the application does not implement function level or role based access control. Instead, access control is enforced at the user and licence level, ensuring that only authorised individuals can access the system in the first place. This model supports strong governance by clearly defining who is permitted to use the application, while maintaining a robust, transparent, and investigator friendly user experience once access is granted.	

3.06	Does security allow for access to be limited to: - Read only? - Read/write? - Read/amend/delete?	The solution applies clear and robust access control at the user and environment level, ensuring that only authorised individuals are able to access the system and work with investigative data. Once access has been granted, authorised users are provided with a consistent and fully featured investigative environment. All users have the ability to create, amend, and manage investigative data within the application, supporting effective end to end investigative workflows without functional constraint. This approach delivers several benefits: Operational effectiveness – investigators are not restricted by fragmented permission models and can work efficiently across the full lifecycle of an investigation. Reduced administrative overhead – there is no requirement to manage complex, granular permission sets (for example, read only vs read/write), lowering the risk of mis configuration.	Noted.
3.06 cont.		Clear accountability – access is tightly controlled by user provisioning and licensing, making it straightforward to evidence who is authorised to use the system. The application does not apply differentiated permission levels such as read only, read/write, or read/amend/delete on a per user basis. Instead, access control is focused on who can access the system, rather than restricting capability once access has been granted. This model supports clarity, consistency, and ease of audit, which are particularly important in investigative and evidential environments.	
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?	The Financial Investigation Toolkit is designed as a self contained investigative application and does not expose data through external reporting interfaces such as ODBC connections or third party report writers. There are no external system connections into the FIT software. All data access, analysis, and reporting activities are performed within the controlled application environment by authorised users. This architecture delivers strong security and assurance benefits: Eliminates external attack surfaces by preventing direct database or reporting tool access. Ensures all data access is governed by application level access controls, user provisioning, and licence entitlement. Removes the need to replicate or re enforce security controls across third party reporting tools or integration layers. Supports auditability and data integrity, as all investigative activity takes place within a single, managed environment.	Confirmed.

3.08	Does the system security integrate with Microsoft's Active Directory or other tools that provide a single sign-on?	The solution supports secure, single sign-on access at the environment level through its use of Microsoft technologies. For cloud-hosted deployments, users access the Financial Investigation Toolkit via a dedicated Windows 11 Cloud PC hosted on Microsoft Azure. Authentication to this environment is managed using Microsoft identity services, allowing organisations to leverage existing Microsoft account controls and standard joiner, mover, and leaver processes. This provides a familiar and secure sign-in experience aligned with Microsoft best practice. Once authenticated to the Windows Cloud PC environment, users can access the Financial Investigation Toolkit without the need for additional application-level credentials. This approach delivers the practical benefits of single sign-on, reducing password fatigue and simplifying user access management.	Noted.
3.08 cont.		The application itself does not maintain a separate internal authentication or role-based access control layer, nor does it directly integrate with on-premises Active Directory for function-level permissions. Instead, security is enforced through: Microsoft-managed user authentication to the Cloud PC or workstation Controlled user provisioning Licence-based access to the application This model provides a secure, streamlined access experience while maintaining clear accountability over who is authorised to access the investigative environment.	
3.09	Does the system provide multi-factor authentication (MFA)?	The solution supports multi-factor authentication at the environment access level through its use of Microsoft technologies. For cloud-hosted deployments, users access the Financial Investigation Toolkit via a Windows 11 Cloud PC hosted on Microsoft Azure. Authentication to this environment is managed using Microsoft identity services, which natively support multi-factor authentication (MFA) in line with organisational security policies. This allows MFA to be enforced as part of the standard Microsoft sign-in process before a user can access the investigative environment . Once authenticated to the Cloud PC environment, users can access the Financial Investigation Toolkit without requiring a separate application-level login. This approach ensures that MFA is applied before access to the system is granted, strengthening overall security while maintaining a streamlined user experience.	Noted.
3.09 cont.		The application itself does not implement a separate, internal MFA mechanism. Instead, it relies on the robust MFA capabilities provided by Microsoft, enabling organisations to apply consistent authentication controls across their wider Microsoft estate.	

Passwords and access logs			
3.10	Is access to the software controlled by password?	No, the application is installed on a users laptop, so access is controlled by access to the laptop. The application only runs locally on that machine.	Confirmed.
3.11	Does each user have a separate log on (user ID)?	Please see 3.10.	Confirmed.
3.12	If there is no password facility please state how confidentiality and accessibility control is maintained within the software?	The application runs within the local users context on their laptop.	Confirmed.
3.13	Are passwords masked for any user logging in?	NA - The user primarily uses the tool to interact with transaction data within Excel. Access to the scan an OCR tools is controlled through access to the Windows login of the computer.	Confirmed.
3.14	Is password complexity available and enforced?	NA	N/A
3.15	How many previous passwords are retained / the password history?	NA	N/A
3.16	Are passwords encrypted?	NA	N/A
3.17	Are users automatically logged off after a pre-set idle time? - Can the time period be changed? - Can any information be viewed without being logged in, including after logging off, if so what information?	NA	N/A
Deletion of transactions			
3.18	Is it possible to delete a transaction?	Yes through native Excel functionality.	Confirmed.
3.19	If so, then how are deletions controlled by the system?	NA	N/A
3.20	Are deleted transactions retained in the audit trail (see below) and denoted as such?	NA	N/A
Audit trails			
3.21	Does the system have an audit trail (log) which records all changes to transactions in the system?	NA - The user primarily uses the tool to interact with transaction data within Excel. Access to the scan an OCR tools is controlled through access to the Windows login of the computer.	Confirmed.
3.22	Does this log also record any system error messages and/or any security violations?	The application does record error logs and messages which can be used by customer or Altia support teams to resolve issues.	Noted.
3.23	Is it possible to turn off or delete the audit trail?	NA	N/A
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?	NA	N/A
3.25	Are all master file changes recorded in the audit trail?	NA	N/A
Compliance			
3.26	Does the system operate in a way that is compliant with data protection legislation including GDPR? How does the system facilitate this?	Yes. The solution allows the organisation to dispose of data inline with GDPR guidance at the end of a contract. Any organisation using the tool must ensure that any data stored for long terms is reviewed through their processes for GDPR.	Noted.
3.27	Describe your use of sub-processors if any?	Microsoft Azure is used to host the solution.	Noted.
Backup and recovery			
3.28	Is there a clear indication in the software or manuals as to how the data is backed-up and recovered?	Yes. If the solution were delivered from the cloud (using Azure Virtual Desktop).	Noted.
3.29	How often are backups taken and to what point can restores be done?	Every night. Instant backups 7 days, data retention 30 days.	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).	The application is not writing data to a database, the data is stored on the file system or within Excel. Therefore saving failures are handled by Windows and Excel natively.	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?	The application allows recovery and partial rescan options in various places to minimise any rework required in the instance of an application failure.	Noted.
3.32	What features are available within the software to help track down processing problems?	Error logs are recorded by the application which can help local user, IT teams and Altia's support team identify the problem.	Noted, see response 3.22.

Ref	Requirement	Response	Reviewer comments
4	**DATA PROCESSING AND REPORTING**		
Input and validation of transactions			
4.01	Is data input controlled by self-explanatory menu options?	Yes. There are various options for inputting and importing data, often controlled by guided wizards.	Confirmed.
4.02	Are these menus user/role-specific?	The menus are licence specific, but due to the nature of the software roles are not required.	Confirmed.
4.03	Can the creation or amendment of standing data (e.g. customer account details) be undertaken using menu options or dialogue boxes as opposed to requiring system configuration?	If this means customer account details from statements or invoices then this is automatically captured by the Toolkit product.	Confirmed.
4.04	Does the software provide input validation checks such as: - [account] code validation? - reasonableness limits? - validity checks?	Yes. There are many levels of validation checks, this is one of the specialist areas of the tool. For example the tool can import many transactions and check balances highlighting suspected incorrect transactions.	Confirmed.
4.05	What control features are within the software to ensure completeness and accuracy of data input?	Yes. There are many levels of validation checks, this is one of the specialist areas of the tool. For example the tool can import many transactions and check balances highlighting suspected incorrect transactions.	Confirmed.
4.06	How does the software ensure uniqueness of the input transactions? (i.e. to avoid duplicate transactions)	Yes the software has advanced transaction matching with multiple methods for detecting duplicate or linked transactions.	Confirmed.
4.07	Is data input by users validated by scripts or routines in the browser, or other client software, before transmission to the server?	No	Noted.
4.08	Is data input by users validated by routines running on the server before data files are updated?	No	Noted.
4.09	Does the above validation ensure that data entryed in all input boxes: - Cannot be longer than a maximum length? - Cannot contain unaccepted characters such as semi-colons etc?	No	Noted.
4.10	Are input errors highlighted?	Yes	Confirmed.
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 to all	Confirmed.
4.12	Are responses to erroneous data input clear so that they do not lead to inappropriate actions?	Yes	Confirmed.
4.13	Does the software have an automatic facility to correct/reverse/delete transactions?	No	Noted.
4.14	If yes, are these logged in the audit trail?	N/A	Noted.
4.15	Are all data entries or file insertions and updates controlled to ensure that should part of a data entry fail the whole transaction fails?	N/A	Noted.
4.16	Are messages provided to users clearly explaining whether the data entry or file upload has been processed successfully or not?	Yes	Noted.
Import and export of data			
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.	Generally, storage is local, unless the users have purchased the cloud option. For the cloud option 1tb of storage is provided, it is unlikely that users will require above that, pricing can be provided if more space were required.	Noted.
4.19	Can data be imported into the system from multiple types of files, e.g. XLS, text, CSV?	Yes, Toolkit (scan and OCR) support multiple images and pdf file types. The Toolbar in Excel supports import from files types that Excel supports.	Confirmed.

4.20	Explain how the system validates imports into the system and what happens to any import which fails?	N/A	N/A.
4.21	Are imported /interfaced transactions detailed in the audit trail? *[See also 3.27]*	As the tool is integrated into Excel audit isn't provided in this way.	Noted.
4.22	Can data be exported from all areas of the system to multiple formats e.g. XLS, CSV, PDF, text; if so specify which formats are supported?	Yes, Toolkit (scan and OCR) support multiple export types typically excel files. The Toolbar in Excel supports export from files types that Excel supports.	Confirmed.
Data processing			
4.23	Does the software ensure that menu options or programs are executed in the correct sequence (e.g. outstanding transactions are processed before month end is run)?	The tool include multiple wizards to walk users through the process, advanced users can also work unaided.	Noted.
4.24	Does the software provide automatic recalculation, where appropriate, of data input? (e.g. VAT)	The tool includes automatic tools like currency converter and inflation calculation.	Confirmed.
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?	As the data is stored in a workbook on your drive you can delete as you need necessary.	Noted.
4.27	What is the size and format of reference numbers and descriptions within: - Ledgers? - Stock? - Currencies?	As the software converts financial statements to Excel Worksheets, the format and reference numbers are the same as the source data.	Noted.
4.28	How does the software guard against/warn about duplicate account numbers on set up?	As the software is an Excel tool, there is no set up.	Noted.
4.29	How does the software enable the traceability [from, to and through the accounting records] of any source document or interfaced transaction?	You can trace across accounts with the transaction matcher tool.	Noted.
4.30	What drill down/around functionality is available within the software?	This depends on the number of analysis tools you have ran on the source data.	Noted.
4.31	If the software uses a lot of standing information which changes frequently or regularly, does the software allow for such changes to be effected through the use of parameters or tables?	Standing Information can be downloaded on an as-hoc basis: currency & inflation data.	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)?	As the software is an Excel Add-in any reports generated from the source data will use Excel functionality.	Confirmed.
4.33	Is the report writer based on a standard SQL-type approach and is it flexible and easy to use?	As the data is stored in an Excel Worksheet and not a database, any reports generated from the source data will use Excel functionality which is easy to use.	Noted.
4.34	Can the report generator operate over the financial and operational aspects of the system, e.g. combining service metrics with financial information?	No	Noted.
4.35	Is a comprehensive data dictionary provided to aid field selection?	We have user manuals included in the software.	Noted.
4.36	Does the system provide a library of reports and templates which can be amended, saved and re-run?	We have a number of standard reports that can be ran, which can not be amended, however as the software layers upon Excel functionality, this can be used to amend existing reports or create your own.	Confirmed.
4.37	Can users create their own reports? If so, what are the controls on users doing this?	Yes, standard Excel functionality.	Confirmed.
4.38	Can users create saved searches/filters/queries?	Yes	Confirmed.
4.39	Can regular reports be added to user menus in the appropriate area of the system?	Yes, using the Pattern Manager functionality.	Confirmed.
4.40	Does the system support the production of on demand (interactive) and scheduled batch reports?	As the software is an Excel tool, there is no functionality to run scheduled reports. You can create reports as and when required.	Confirmed.

Ref	Requirement	Response	Reviewer comments
5	**USABILITY**		
Ease of use			
5.01	Does the solution provide a multi-language user interface?	Yes. The solution provides a multi language user interface to support international and multi lingual user communities. The Financial Investigation Toolkit is available in the following languages: English Spanish French This enables organisations to deploy the solution across teams operating in different regions or language environments, improving usability, adoption, and consistency of investigative processes. The availability of multiple interface languages supports inclusive working practices while maintaining a consistent feature set and user experience across all supported languages .	Confirmed, see question 7.45.
5.02	Does the system allow for customisable branding and UI (e.g. corporate colour palette, upload company logo, etc)?	The solution provides a standardised and consistent user interface across all deployments. Customisable branding elements, such as corporate colour palettes, customer logos, or bespoke UI theming, are not supported within the product. The interface is delivered as a consistent, pre configured experience for all users. This approach offers several practical benefits: Consistency and usability – all users experience the same interface, reducing training effort and supporting rapid user adoption. Operational stability – avoiding UI customisation reduces complexity and the risk of introducing usability or support issues. Simplified maintenance and upgrades – a standard interface ensures that updates and enhancements can be deployed efficiently without customer specific rework.	Confirmed.
5.02 cont.		The focus of the solution is on providing a robust, secure, and highly functional investigative environment, rather than UI branding customisation, ensuring reliability and consistency across the user base .	

5.03	Does the system have a similar look and feel and overall consistency between screens and modules?	Yes. The system provides a consistent look and feel across all screens and modules. The Financial Investigation Toolkit follows established Microsoft Windows user interface standards, ensuring a familiar and intuitive experience for users. This is particularly evident where the solution is integrated with Microsoft Excel, as the toolkit adopts standard Microsoft conventions for menus, toolbars, navigation, and interaction patterns . This approach delivers several benefits: Consistency and usability – users experience a coherent interface across all areas of the system. Reduced training overhead – familiarity with Microsoft Windows and Excel significantly shortens the learning curve. Improved user adoption – investigators can work confidently within an interface that aligns with tools they already use daily. Overall, the solution's adherence to Microsoft UI standards ensures a predictable, professional, and user friendly experience throughout the application.	Confirmed.
5.04	Is data entry easily repeated if similar to previous entry?	Yes, one of the key concepts of the product is to significantly increase speed of data entry for financial transactions.	Confirmed.
5.05	Does the software prevent access to a record while it is being updated?	No this is not available in the product.	Noted.
5.06	Is there locking at file or record level?	No this is not available in the product.	Noted.
5.07	Does the software allow for the running of reports whilst records are being updated?	Yes, the product can run reports based on the data available.	Confirmed.
5.08	Can timestamps or user comments be added to transactions?	Yes, the main data is stored within Excel so normal Excel interaction is available.	Confirmed.
5.09	Is there the ability to store preferences and default values on a per-user basis e.g. department/team/user?	Yes this is included within the product. For example pattern matching rule files can be saved for individuals and shared with other users as required. Altia also provides a community set available to all customers.	Confirmed.
5.10	Does the system have the ability to provide user-defined fields with associated validation of data input?	Yes, the reports can be configured by users	Confirmed.
5.11	Can the system provide users with reminders and notifications e.g. workflows?	The application has a number of wizards and screen that walk users through the processes guiding users where necessary.	Noted.
5.12	If the system provides workflows, does it have functionality to substitute/delegate authorisations?	This is not required in the application workflow.	Noted.
5.13	Describe the tools and features available for a power user to make configuration changes such as amending a workflow.	Users, for example using the pattern manager functionality, can create their own rule files allowing customisation of how the product looks for transactions.	Noted.
5.14	Is there the ability for users to define and configure layouts of letters and forms?	Yes, there are set of layouts that can be configured and defined by the users.	Noted.
5.15	Can users save the parameters of searches?	Yes, and there are a set of predetermined searches, filters and reports.	Confirmed.
5.16	Does the system have a "universal search" option, allowing a search to be undertaken over all modules of the system?	Yes using built in functionality within Excel.	Confirmed.

5.17	Can the system store menu option 'favourites' on a per user basis?	Yes. The system allows users to store menu option "favourites" on a per user basis. This functionality enables individual users to personalise their working environment by saving frequently used tools or menu options for quick access. User specific favourites improve efficiency by reducing navigation time and supporting streamlined investigative workflows, particularly for users who regularly rely on a consistent subset of functionality. This capability enhances usability while maintaining a consistent underlying user interface and does not introduce additional security or configuration complexity, as favourites are managed at the individual user level within the application environment.	Confirmed.
5.18	Can a user open multiple windows accessing the same or different modules of the system?	Yes. The system allows users to open and work with multiple windows concurrently, accessing the same or different modules of the application. This capability enables users to: View and compare information side by side Work across different areas of the system simultaneously Maintain context when switching between investigative tasks Supporting multiple open windows enhances productivity and reflects standard Microsoft Windows behaviour, providing users with a flexible and efficient working environment that aligns with familiar desktop application usage patterns.	Confirmed.
5.19	Can more than one software function be performed concurrently?	Yes. The system allows more than one software function to be performed concurrently. Users can work across multiple functions at the same time, for example running analysis, reviewing data, and preparing reports in parallel. This capability supports efficient investigative workflows and reflects standard Microsoft Windows application behaviour, particularly where the solution operates within or alongside Microsoft Excel. Enabling concurrent activity improves productivity, reduces task switching, and allows users to progress multiple strands of work without interruption, which is especially valuable in complex or time critical investigative scenarios.	Confirmed.

User documentation and training			
5.20	Confirm whether a user manual / instructions is provided and how this is distributed?	Yes. The solution provides user manuals and instructions, which are available directly within the product. This ensures that users have immediate access to guidance and reference material as part of their normal workflow, supporting effective day to day use of the system. In addition to in product user guides, further training and support services are available through Altia's dedicated support and training teams. This enables organisations to supplement self service documentation with structured training, onboarding support, and ongoing assistance as required, ensuring users can maximise the value of the solution throughout its lifecycle.	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?	Yes. The user manual provides comprehensive coverage to support effective use of the system and is designed to meet both new and experienced user needs. The user documentation includes: An index and search facility, enabling users to quickly locate relevant guidance. Clear guidance on basic software functions, supporting onboarding and day to day use. Screenshots and illustrations of screens and layouts, helping users easily relate instructions to the live system. Worked examples, demonstrating how common tasks and investigative activities are performed. Tutorial content, supporting structured learning and skill development. Details of error messages and their meanings, assisting users in understanding and resolving issues efficiently.	Noted.
5.21 cont.		These materials are available directly within the product, ensuring contextual, on demand access. They are also accessible via a training portal, which complements the in product documentation and supports ongoing learning, refresher training, and user development. Further assistance is available through Altia's support and training teams as required, providing a robust and well supported user enablement model.	
5.22	Is context-sensitive help available within the system?	No this is not available in the product.	Noted.

5.23	Is the manual and/or help editable by the user (subject to the permissions matrix)?	By default, the user manual and in product help content are not editable by end users. This ensures consistency, accuracy, and control over core product guidance. However, under a Non Disclosure Agreement (NDA), Altia can provide customers with editable versions of selected training guides and manuals. This allows organisations to tailor supporting materials for their own internal use, for example to apply corporate branding, align language to internal processes, or incorporate organisation specific guidance. This approach balances: Controlled, consistent in product documentation for all users, and Flexible customer enablement, where branded or tailored training materials are required outside the core application. Editable content provided under NDA is intended specifically for training and guidance purposes, rather than modification of the in product help system itself.	Noted.
5.24	Will the Software House make the detailed program documentation (e.g. file definitions for third party links) available to the user, either directly or by deposit with a third party (ESCROW)?	Yes. Altia will make detailed programme documentation available and can support a software escrow arrangement at the customer's cost. Where required, escrow can be established with a recognised third party provider (for example, NCC Group), providing independent assurance and long term risk mitigation. The scope of materials placed into escrow would be agreed contractually as part of the escrow arrangement.	Noted.
5.25	Please detail the training options available?	Training options available Altia offers a flexible training model that supports self service learning, structured instructor delivery, and customer specific enablement for the Financial Investigation Toolkit (FIT) and related investigation solutions. 1) Digital eLearning (on demand, self paced) Structured online modules designed for learning at your own pace, suitable for onboarding and ongoing development. FIT training is available in on demand formats, with content that can be revisited over an access period (e.g., the FIT training page references self paced e learning content). [altiaintel.com] Altia also provides access to an e learning site as part of its wider user enablement approach. 2) Free video tutorials (self guided) On demand videos to support familiarisation with key features and concepts, including availability for FIT.	Noted.

5.25 cont.		3) Trainer led virtual classroom courses (live online) Interactive, trainer led sessions delivered remotely, focused on practical workflows and real use cases (available for FIT and other Altia products). 4) Trainer led onsite classroom courses (live in person) Instructor led delivery at customer premises, tailored to organisational workflows and investigative context (the training page explicitly positions in person training as tailored to the organisation and context). 5) Bespoke courses customised to an individual customer Customer specific training can be shaped around operational priorities and investigative context; the FIT training page describes premium training as customised to organisational requirements (including a pre training assessment) and delivered in closed sessions either in person or online.	Noted.

5.25 cont.		6) Train the trainer options Designed to enable nominated "key users" to share knowledge internally and embed consistent ways of working; the training page explicitly describes this as an available approach. 7) Ongoing support wrap (to reinforce training outcomes) Training is complemented by ongoing support from Altia teams, and Altia's training team can provide further courses (noting that additional training courses can be provided for an additional fee). Altia also runs annual user groups as a forum for updates, feedback, Q&A, and knowledge sharing across the investigator community.	Noted.
5.26	Who provides training: - Software House? - VAR?	Altia provides all training directly to customers. Training is delivered by Altia's accredited trainers, who have specialist product knowledge and practical investigative experience. Training is not delivered via a VAR. This ensures consistency, quality, and alignment with product updates, best practice workflows, and evidential standards, with training delivered by the Software House responsible for the solution.	Noted.
Support and maintenance			
5.27	How is the software sold: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	The software is sold both directly by Altia and via approved Value Added Resellers (VARs) and integrators. Customers can procure the solution direct from the Software House (Altia), or through established VAR and integrator partners, including organisations such as Phoenix, Computacenter, and Insight. This provides flexibility to align procurement with existing commercial frameworks, purchasing routes, and preferred suppliers, while ensuring the solution and support remain backed by Altia.	Noted.
5.28	How is the product supported: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	All support services are provided by the Software House (Altia) through its dedicated support organisation. Support is not delivered via a Value Added Reseller (VAR) or integrator, ensuring customers have direct access to product specialists with in depth technical and operational knowledge of the solution. This direct support model provides clear accountability, faster issue resolution, and assurance that support remains aligned with product updates, security standards, and best practice.	Noted.
5.29	Do VARs have to go through an accreditation process?	Altia works with approved and accredited VARs and integrators to ensure they meet defined standards around capability, product knowledge, and delivery quality. This approach ensures customers receive a consistent and reliable experience regardless of the procurement route, while maintaining Altia's quality, security, and governance standards.	Noted.

5.30	Is the software sold based upon number of named users or a number of concurrent users?	The software is licensed flexibly and can be sold using multiple licensing models, depending on the option selected. Altia supports: Named user licences, assigned to specific individual users. Concurrent user licences, allowing a defined number of users to access the software at the same time. Workstation (computer based) licences, where the licence is tied to a specific device rather than an individual user. This range of licensing options enables customers to select the most appropriate and cost effective model based on how the software will be accessed and used across their organisation.	Noted.
5.31	The supplier should detail the support cover options available, covering: - The hours provided? - Associated costs? - The global regions covered?	Altia provides direct support , ensuring customers have access to experienced product specialists with in depth technical and operational knowledge of the solution. Hours Provided Standard support is provided during business hours, with enhanced or extended support options (including out of hours cover) available where required. Support hours and response targets are defined contractually and can be aligned to the criticality of the service and customer operational needs. Associated Costs Support is typically included as part of the annual support and maintenance agreement. Where customers require enhanced service levels, extended hours, or bespoke support arrangements, these can be provided at an additional agreed cost, tailored to the required level of coverage and service assurance. Global Regions Covered Altia provides support to customers globally, supporting deployments across the UK, Europe, North America, and other regions. Support delivery is structured to align with customer geography and operational requirements, ensuring consistent service regardless of location.	Noted.

5.32	Detail the process by which customers raise support requests and how these can be viewed/managed?	Customers can raise support requests using two primary channels, providing flexibility and ease of access. Support tickets can be raised directly from within the system, enabling users to log issues in context while working with the product. This helps ensure accurate information is captured and supports efficient triage by the Altia support team. Support requests can also be raised via an online support portal, which provides a central point for logging, tracking, and managing tickets. Through the portal, users can view the status of open requests, review updates and responses from Altia, and maintain a clear audit trail of all support interactions. This dual channel approach ensures: Simple and accessible issue reporting for users Transparency and visibility of ticket status and progress Effective management and communication throughout the support lifecycle All support requests are handled directly by Altia's support organisation, ensuring continuity, accountability, and access to specialist product expertise.	Noted.
5.33	Please note the methods of support available: - Telephone? - Internet chat? - Remote access to customer workstation? - Other, please specify?	Methods of Support Available Altia provides support directly through the Software House, delivered by dedicated support teams to ensure consistent service quality and product expertise. Telephone support Available via Altia's support organisation, with primary coverage provided by the UK support team, and in region support for customers where required. Internet chat Support is available through an online support portal, which includes chat functionality for real time assistance and issue resolution. Email support Customers can raise and manage support queries via email, integrated with the support portal to ensure tracking and auditability of requests. Remote access to customer workstation Where required and subject to customer approval and security controls, Altia can provide remote support sessions to assist with diagnosis and resolution of issues.	Noted.

5.34	Do you offer service credits for failure to meet performance around SLA and uptime (if applicable)	Yes. Altia publishes Service Level Agreements (SLAs) as part of its standard customer contracts. SLAs define performance measures for service delivery, including response times and service availability where applicable. Any remedies, including the applicability of service credits for failure to meet agreed SLA targets or uptime commitments, are set out contractually within those SLAs and aligned to the specific services being provided. This approach ensures transparency, clear expectations, and appropriate commercial protections, with SLA terms tailored to the nature and criticality of the deployed solution.	Noted.
5.35	What is your escalation path for tickets which have not been resolved within a reasonable time?	Altia operates a formal escalation policy, which provides customers with a clear and structured route to escalate support issues where resolution has not been achieved within a reasonable or agreed timeframe. The escalation process is: Documented and governed as part of Altia's information security and service management framework. Reviewed and assured under ISO 27001, ensuring that escalation handling, accountability, and governance are formally defined and regularly audited. Where escalation is required, tickets can be progressed through defined support management levels, ensuring increased visibility, priority, and senior oversight as appropriate. Customers are kept informed throughout the escalation process, with clear ownership and communication until resolution is achieved. This approach ensures transparency, accountability, and effective issue resolution, while providing customers with confidence that robust controls are in place should escalation ever be required.	Noted.
5.36	How often are general software enhancements provided?	General software enhancements are provided on a regular release cycle, with typically three to four software releases per year. These releases include a combination of functional enhancements, usability improvements, and ongoing maintenance updates, ensuring the solution continues to evolve in line with customer needs, regulatory requirements, and technology advancements. Software updates are delivered as part of Altia's standard support and maintenance arrangements.	Noted, see question 7.82.
5.37	Will they be given free of charge?	Yes. General software enhancements are provided free of charge to all customers who hold an active support and maintenance agreement. All customers in support receive software updates and enhancements as part of the standard service, with no additional licence or upgrade fees for these releases. This ensures customers benefit from ongoing product improvements, new functionality, and maintenance updates throughout the support term.	Noted.

5.38	How are enhancements and bug fixes provided to customers?	Enhancements and bug fixes are provided as part of Altia's standard release process. For on premise or locally installed deployments, updates are delivered through new installation files, which customers use to apply the latest version of the software. This ensures customers can control the timing of updates in line with internal change management processes. For cloud hosted customers, enhancements and bug fixes are automatically applied by Altia as part of the managed service. This ensures customers are always running the latest, supported version of the software without the need for manual intervention, while maintaining service continuity and security. This dual approach provides flexibility for customers with different deployment models, while ensuring all customers benefit from ongoing improvements and fixes as part of their support entitlement.	Noted.
5.39	Is "hot line" support to assist with immediate problem solving available?	Telephone line support is provided during UK business hours where our experienced support team are available to assist customers.	Noted.
5.40	If so, is there an additional cost involved?	No.	Noted.
5.41	At what times will this support be available?	Telephone line support is available during UK business hours. During these times, Altia's experienced support team is available to assist customers with immediate problem solving and operational queries. Support is delivered directly by Altia, ensuring access to knowledgeable product specialists.	Noted.
Integration and www facilities			
5.42	Are the different modules of the system fully integrated (i.e. no set-up effort required in order to use the various modules together)?	Yes. The different modules of the system are fully integrated. Altia's solution is designed as a cohesive platform, with modules built to work together seamlessly. Where multiple modules are deployed, they integrate natively, allowing customers to use them together without the need for separate configuration or additional setup effort. This ensures a consistent user experience and supports efficient workflows across the system.	Confirmed.
5.43	Are they integrated on real time basis or batch basis?	In the main real-time. Output from the Investigation Toolkit product is exported to the file system and immediately available to the Investigation Toolbar product. Additional API based integration is available to other Altia products.	Confirmed.

5.44	Can the software be linked to other packages e.g. word processing, graphics, financial modelling, to provide alternative display and reporting facilities?	Yes. The software can be linked to other packages to support alternative display and reporting facilities. Altia provides direct integration with Microsoft Excel through the Altia Investigation Toolbar, which operates as an Excel add in. This allows users to analyse, model, manipulate, and present investigative data using familiar spreadsheet, financial modelling, and reporting capabilities within Excel. For cloud hosted deployments, integration with Microsoft Power BI is available. This enables customers to create advanced visualisations, dashboards, and analytical reports using Power BI, supporting alternative views and presentation of investigative data beyond standard in application reporting. This approach allows customers to leverage widely adopted Microsoft productivity and analytics tools alongside Altia's investigative functionality, enhancing reporting flexibility without the need for bespoke integration work.	Confirmed.
5.45	Can definable links to spreadsheets be created?	Yes. Definable links to spreadsheets can be created. Altia enables users to work directly with spreadsheets through its integration with Microsoft Excel, including the ability to create and manage links between investigative data and Excel workbooks. This supports flexible analysis, modelling, and reporting using familiar spreadsheet functionality as part of the investigative workflow.	Confirmed.

5.46	Does the system provide a secure document storage capability: If so, please give examples of the document types saved and what transactions these might relate to.	Yes. The system provides secure document storage at a transaction level. Each transaction within the system can have supporting documentation securely attached, allowing evidential material to be stored, managed, and accessed in direct context with the relevant financial record or investigative entry. Examples of document types that can be attached include: Bank statements and transaction records Invoices and receipts Scanned documents and correspondence Cheque images Notes and investigator generated documents These documents are typically linked to individual financial transactions, enabling users to associate evidential material such as proof of payment, source documentation, or explanatory notes directly with the transaction they relate to. This supports clear audit trails, evidential integrity, and efficient case review within a secure environment.	Confirmed.
5.47	Can documents be scanned into a secure repository?	The system does not provide native, direct document scanning functionality (i.e. it does not connect directly to physical scanners). However, documents that have been scanned outside the system (for example, using a standard scanner to create PDF or image files) can be securely uploaded and attached within the system, including being linked directly to individual transactions. For cloud hosted deployments, this upload and attachment capability is provided within the secure hosted environment, allowing scanned documents to be stored and managed securely once digitised. This approach ensures: Scanned documents are stored securely within the system Documents can be linked directly to relevant transactions Customers retain flexibility to use their existing scanning hardware and processes	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?	Yes. The system provides defined connection mechanisms through built in APIs, with controlled scope and purpose. The software includes specific API integrations designed to enrich investigative analysis rather than provide unrestricted system to system connectivity. These APIs are used to retrieve external reference data and automatically apply it within the application. Connection Mechanisms The system supports API connections to trusted external data sources, including: Companies House data – to enrich entity and company information. Inflation data – to support financial calculations and historical value analysis. Currency conversion data – to normalise and analyse transactions across different currencies.	Confirmed.
5.49 cont.		Breadth of Functionality These integrations are primarily read only in nature. Data retrieved via APIs is used within the system for analysis, calculation, and reporting, rather than allowing external systems to add, update, or delete core system records. Core investigative data and transactions remain managed and controlled within the application, preserving data integrity and evidential assurance. Third Party Connectivity The system does not expose open, general purpose web service APIs that allow customers to connect arbitrary third party software to perform unrestricted operations (add, update, delete) on system data. Integration is intentionally controlled and purpose specific, reducing security risk and maintaining governance over sensitive investigative data. This approach balances integration capability with security, evidential integrity, and operational assurance.	
5.50	Does the system support mobile working?	Yes. The system supports mobile working in a laptop context. The application can be used on any supported laptop while on the move and does not require an active internet connection to operate. This allows users to continue working in environments where connectivity may be limited or unavailable, supporting flexible and resilient investigative workflows. Mobile phone or tablet working is not supported, and the solution is not designed for use on handheld mobile devices. This approach ensures full functionality, performance, and evidential integrity are maintained while enabling portable, offline use on approved laptop devices.	Noted.

Ref	Requirement	Response	Reviewer Comments
6	SaaS HOSTING		
	This evaluation covers the system but not the method by which it is delivered and/or contracted for. Potential users need to satisfy themselves on the security and disaster recovery aspects and licensing of the online system and any data protection issues of their own and customer/supplier information, contained therein, being held on the system, as well as the return of the data when the contract expires or is terminated.	Altia provides two delivery methods for the application. It can be installed on-premise on users' local computers, or it can be delivered from the cloud using Altia managed Azure Virtual Desktop. The answer below refer to customer who have purchased the cloud deployment option.	
Data			
6.01	Whose data centres are used and where are these located: - If hosted -- where data centre controlled by a third-party? - If SaaS -- where the software vendor will be in control?	Hosted / SaaS Deployment For hosted and SaaS deployments, the solution is hosted on Microsoft Azure, using Microsoft owned and operated data centres. In this model, the underlying data centre infrastructure is controlled by Microsoft, a global hyperscale cloud provider, while Altia retains control of the application, configuration, and service delivery. Data Centre Locations Data centre location is aligned to customer and regulatory requirements. For UK public sector customers, services are typically hosted within UK Azure regions, ensuring data residency and compliance with UK data protection and security expectations. Other regions can be supported where required, subject to contractual agreement. Control Model Summary	Noted.
6.01 cont.		Third party data centres: Microsoft Azure (physical infrastructure and facilities) Software vendor control: Altia controls the application, security configuration, access management, and service operations SaaS responsibility: Altia is responsible for operating and supporting the SaaS service on Azure This shared responsibility model combines the resilience, scale, and certification of Microsoft Azure with Altia's application level governance, security, and operational control.	

6.02	Does the customer get a choice of the jurisdiction in which their data resides?	Yes. Customers are given a choice of the jurisdiction in which their data resides. Data residency is determined by customer location and regulatory requirements, and customers can select from supported regions. Altia currently supports data hosting in the United Kingdom, Australia, and the United States, ensuring alignment with local data protection, sovereignty, and compliance obligations. Data is hosted within the selected jurisdiction for the duration of the service.	Noted.
6.03	What certification(s) do you or your platform operators hold relating to your data centres and your business operations?	Altia (Software Vendor – Business Operations) Altia operates under recognised information security standards to ensure robust governance, risk management, and protection of customer data. ISO/IEC 27001 – Altia is certified to ISO 27001, covering its information security management system, policies, processes, and operational controls. Cyber Essentials Plus – Altia holds Cyber Essentials Plus, providing independent assurance of protection against common cyber threats. Platform Operator / Data Centres (Cloud Infrastructure) For hosted and SaaS deployments, Altia uses Microsoft Azure, where the physical data centres and underlying infrastructure are operated by Microsoft. Microsoft Azure data centres hold a wide range of internationally recognised certifications, including: ISO/IEC 27001 (Information Security Management) ISO/IEC 27017 (Cloud Security Controls) ISO/IEC 27018 (Protection of Personal Data in the Cloud) SOC 1, SOC 2, and SOC 3 reports PCI DSS (where applicable)	Noted.
6.03 cont.		These certifications provide assurance over the physical security, resilience, and operational controls of the data centre environment, while Altia remains responsible for application level security, configuration, and service operations.	Noted.

6.04	Do you or your platform operator have an SSAE16 (System and Organisation Controls) report available?	Yes. An SSAE 16 / SOC report is available via our platform operator. For hosted and SaaS deployments, Altia uses Microsoft Azure as the cloud platform. Microsoft provides SOC 1 Type II reports (which replaced SSAE 16 under SSAE 18) covering the controls relevant to financial reporting and operational assurance for its cloud services. These reports are independently audited and made available by Microsoft under NDA. Altia itself does not publish a standalone SSAE 16/SOC 1 report for its business operations. Instead, Altia operates under ISO/IEC 27001 certified information security management, with application level controls and processes audited accordingly, while relying on Microsoft's SOC reports for infrastructure level assurance. This model provides customers with: SOC assured cloud infrastructure (Microsoft Azure) ISO certified application and service operations (Altia)	Noted.
6.05	What are the physical controls over the:- - Premises? - Fileservers? - Communications equipment?	Altia uses Microsoft Azure for hosting cloud applications. Both Microsoft and Altia hold ISO27001 which covers certification for premise security arrangements.	Noted.
6.06	Is the space in this/these data centre(s) shared with any other companies?	If the cloud version is chosen for a customer they have their own dedicated tenant within Azure.	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?	For cloud customers separation is provided at an Azure tenant level.	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?	For cloud customers, customers are separated by tenant with only users from that customer given access to the tenant. This is identifiable on login screens using customer logos and dedicated domain names.	Noted.
6.09	What controls are in place to prevent users from one customer/company accessing data from another customer/company by accident or by design?	User accounts are not shared across customers.	Confirmed.
6.10	How is [Internet] communication traffic monitored to identify potential problems before they happen: - From a performance perspective? - From a security standpoint?	Altia uses multiple tools (for example Application Insights and Azure Sentinel) to monitor network and applications within Azure.	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?	For cloud customers the application runs through Azure Virtual Desktop, the desktop continues running even if the user were to lose their internet access to it. When they reconnect the application will be there as before.	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?	Yes all connections run over encrypted connections using TLS 2.1 or higher.	Noted.
6.13	Is data on your servers encrypted at rest?	For cloud customers yes all data is encrypted at rest.	Noted.
6.14	What level of encryption is used?	AES 256	Noted.
6.15	Is a staging environment provided that is an exact replica of production; which can be used for testing purposes?	A staging environment is not provided and is not consider appropriate for this software given how it is installed. Users can easily uninstall a version of software and reinstall a previous version if required.	Noted.

6.16	Is a test environment provided to test configuration changes? If so, is there an additional charge for this?	A testing environment is not provided and is not consider appropriate for this software given how it is installed. Extensive testing is carried out before the software is released to customers.	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?	Altia adhere to all relavent legislation relating the hosting the application. Access to information is given on a strictly role and need basis, ensuring that data is protected, and only accessed when required for delivering the service.	Noted.
6.18	Are you subject to any legal or regulatory requirements obliging you to retain a copy of customer data?	As a data sub processor for customer Altia adheres to all legal requirements. We are not generally required to hold customer data for longer than the customer contract.	Noted.
6.19	Who will be able to access or see customer data?	If cloud hosted Altia's support and engineering teams can access customer environment for the purposes of resolving support queries or updating software. All relevant Altia staff are NPVV3 and SC cleared as a minimum. Strict ISO27001 audited processes are in place to control access and ensure that environment are only access when required and for the minimum period.	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.	Access is controlled by individual user accounts and only for required roles. Extensive use of PIM (Privileged Identity Management) is used to ensure that access is logged and privilege elevation is only for the minimum period.	Noted.
6.21	Explain the release management procedures in place and the associated segregation of duties ?	Altia follow a standard Agile Software Delivery Life Cycle and have dedicated product management, development and testing teams. Releases go through multiple automated steps before release including automated unit and functional testing, automated security scanning and testing. Finally the QA and Products teams sign off a release to ensure that the product functionality and quality meets the high standards we drive.	Noted.
6.22	Is there sufficient segregation of duties preventing system developers from accessing and changing live applications and data files?	Access is controlled by individual user accounts. Extensive use of PIM (Privileged Identity Management) is used to ensure that access is logged and privilege elevation is only for the minimum period.	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?	Altia's change management is audited under ISO27001.	Noted.
6.24	Is an audit trail always maintained of these emergency changes?	Yes, as part of the ticket details and automated logging for environment access.	Noted.
6.25	What procedures are in place when members of staff leave to ensure that their system access is stopped?	Automated JML process are implemented with accounts automatically being blocked and then removed when a staff member leaves.	Noted.

Platform and service levels			
6.26	Which databases and servers are used to host the software?	Altia uses Microsoft Azure for hosting cloud applications.	Noted.
6.27	What forms of user authentication are supported e.g. user names, passwords certificates, tokens etc.?	Authentication is through EntraId which multiple options of MFA provided.	Noted.
6.28	What is the proposed product/service availability percentage?	Altia provided a 99.9% SLA.	Noted.
6.29	What percentage availability has been achieved over the past 12 months?	Altia has exceeded 99.9% throughout the last 12 months.	Noted.
6.30	Is a service level agreement ("SLA") offered regarding: - Service availability? - Data recovery?	Yes. Details are provided in customer contracts.	Noted.
6.31	Is the service available 24x7 or are there downtime periods for maintenance?	There are small periods of downtime when new releases are installed.	Noted.
6.32	Is the customer made aware of maintenance periods in advance?	Yes customers are given notification of a new release coming out.	Noted.
6.33	Does the application software:- - Require any client software to be installed on the user's computer? - Work entirely within Internet Browser software on the user's computer?	For cloud customers the application can be access through a browser, alternatively users can access it through the Windows App https://apps.microsoft.com/detail/9n1f85v9t8bn?hl=en-GB&gl=GB.	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?	For on-premise customers users (or IT Admin) can download the software for install from Altia's support portal. The software has been digitally signed through DigiCert.	Noted.
6.35	Does the product/service currently use any technologies which are obsolescent / out of support / soon to be end of life? If so, describe how the user can mitigate this risk.	No	Noted.
Platform security			
6.36	What security steps are taken to prevent and detect intrusion attempts?	Altia uses Azure Sentinel and built in Azure protections to monitor access, logging invalid or risk signins. Additionally we have an external 247 SOC which monitors Altia's infrastructure for intrusion attempts.	Noted.
6.37	Is firewall hardware and software used to protect the live systems from unauthorised access?	Yes Azure provides this for AVD.	Noted.
6.38	Which monitoring software is used to create alerts when intrusion attempts are suspected?	Azure Sentinel and Huntress.	Noted.
6.39	Are designated staff responsible for receiving and urgently responding to these alerts?	Yes Altia has a 24/7 SOC.	Noted.
6.40	Have clear procedures been established for identifying and responding to security incidents?	Yes these are audited through ISO27001.	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, updates are applied continually and monitored through multiple tools including ESET and ConnectSecure, and Azure Defender for Cloud.	Noted.
6.42	List the procedures and software tools in place to prevent or detect and eliminate interference from malicious code, such as viruses?	Multiple tools are in place including ESET and ConnectSecure, and Azure Defender for Cloud.	Noted.
6.43	Is a system log maintained by the service provider that details - User access? - User activity? - Error messages? - Security violations?	Yes these are recorded within EntraId.	Noted.
6.44	Is this log available to the customer?	Customer logs can be made available to customers.	Noted.
6.45	Have there been any successful unauthorised access attempts been made during the last year? If Yes:- - What was the effect on the business and users? - What steps are in place to prevent this happening again?	No.	Noted.
6.46	Is penetration testing regularly carried out by (please indicate frequency of tests): - Staff specialising in this field? - External specialists?	Altia carried out an external ITHC with CHECK registered provider annual. This is along side internal automated scanning across applications.	Noted.

6.47	Are procedures in place to ensure that any weaknesses found by penetration testing are addressed quickly?	Yes, Altia has strict polices (audited by IS27001) that ensure that vulnerabilities are rectified appropriately.	Noted.
6.48	If penetration testing by a specialist is not performed regularly, please indicate the main procedures in place to identify weaknesses?	Penetration testing is carried out regularly. Altia also relies on Microsoft's certification and testing for Azure Virtual Desktop.	Noted.
6.49	Are security procedures regularly reviewed? Please indicate frequency of reviews.	At least annually inline with IS27001 requirements.	Noted.
6.50	What security reporting is provided demonstrating compliance against certification(s) and policy(ies)?	Altia holds ISO27001, CE, CE+, irap certifications. Each of these audits our reporting requirements against the certifications.	Noted.
6.51	How are security breaches communicated to customers?	Any security breaches would be communicated through the normal support channels (email, support portal, phone) to registered contacts.	Noted.
Backups by the service provider			
6.52	In relation to backups undertaken by the system provider please explain: - How is a customer's data backed up? - How often is this undertaken? - What is backed up? - What's the media used? - Where are backups stored? - How many copies are there? - How long are they retained for? - Who has access to them? - Is the data encrypted?	For cloud customers backups are automatically carried out every night. Instant recovery backups 7 days, data retention 30 days. The whole users Azure Virtual Desktop is backup including any data stored on it. The data is encrypted using AES 256.	Noted.
6.53	How frequently is a test-restore of backups undertaken?	Our externally audited DR process covers restore of backups. Multiple environment resource are carried out weekly across our estate of servers and environments.	Noted.
6.54	Can the provider restore from a backups that it has taken at a customer request?	Yes through a support request.	Noted.
6.55	Does a customer have the ability to undertake their own backups?	Yes data can be taken out of the evironment and stored elsewhere by the customer.	Noted.
6.56	If so, can a customer restore data a backup that they have taken?	Yes they can copy data back into the environment.	Noted.
Platform recovery			
6.57	What contingency plans are in place to enable a quick recovery from: - Database or application software corruption? - Hardware failure or theft? - Fire, flood and other disasters? - Communication failures?	Altia has extensive business continuity and disaster recovery plans in place which are independantly audited through ISO27001.	Noted.
6.58	How often are these plans tested?	Table top exercises are carried at least annually.	Noted.
6.59	How often are these plans reviewed and updated?	At least annually inline with IS27001 requirements.	Noted.
6.60	What is the longest period of time envisaged that service may not be available?	Altia offers a 99.9% SLA.	Noted.
6.61	What are your: - Recovery Point Object (RPO) standards? - Recovery Time Objective (RTO) minimum standards?	RPO 24 hours. RTO 8 hours.	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?	Not application due to the nature of the application.	Noted.
6.63	What protection is in place to enable users to able to access their accounting and other data if the service provider should experience serious difficulties, cease trading or decide to stop providing the service?	Software can be put into Escrow if required at additional cost.	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?	Software can be put into Escrow if required at additional cost. Notification of data retrival will be provided prior to customer contract end dates.	Noted.
6.65	If the system is hosted are there arrangements in place for this third party to continue providing a hosting service in the short term to allow time for customers to negotiate their own arrangements? If so, how long does the arrangement allow?	Software can be put into Escrow if required at additional cost.	Noted.
6.66	Are there any individual members of the vendor's staff whose leaving or illness would significantly reduce, or even stop, the service provider’s ability to provide a full and reliable service to customers?	No, we have great coverage across teams and DR and BR processed audited by ISO27001.	Noted.
Platform change management			
6.67	Describe your approach to upgrades including what option customers have not to take upgrades (if any)?	Releases are produced 3-4 times per year. On prem customers are responsible for their own installs. Support is provided on the latest and latest -1 versions, meaning that customer may need to upgrade to get software fixes. For cloud customers, they are automatically upgrade post software release.	Noted, see question 7.82
6.68	Are users able to test the application before new versions go into live use?	For cloud environments updates are deployed automatically post release. For on-premise customers local IT teams can control which machines they rollout software to.	Noted.
6.69	Are users given notice before application changes are applied to the live system?	Notifcations are sent to all customers when a new release is available with details of the changes in that release in the form of release notes and builitins.	Noted.
6.70	Are changes delivered into the live environment "switched off" to enable users to test them before enabling them for their environment?	For cloud environments updates are deployed automatically post release. For on-premise customers local IT teams can control which machines they rollout software to.	Noted.
6.71	Describe what testing and QA processes are undertaken before upgrades and other changes are made live/available to customers?	Altia follow a standard Agile Software Delivery Life Cycle and have dedicated product management, development and testing teams. Releases go through multiple automated steps before release including automated unit and functional testing, automated security scanning and testing. Finally the QA and Products teams sign off a release to ensure that the product functionality and quality meets the high standards we drive.	Noted.
6.72	Explain the release management procedures in place and the associated segregation of duties?	Altia follow a standard Agile Software Delivery Life Cycle and have dedicated product management, development and testing teams. Releases go through multiple automated steps before release including automated unit and functional testing, automated security scanning and testing. Finally the QA and Products teams sign off a release to ensure that the product functionality and quality meets the high standards we drive.	Noted, see question 7.82.
6.73	Are users informed when they next login of the application changes that have gone into live use?	Yes	Noted.
6.74	Do customer staff have to take any action (e.g. regression testing) when new editions, patches or upgrades are released? If so, please describe what they should ordinarily do.	We go through multiple steps in our quality assurance process to ensure the high quaility of the software is maintained, but we would always suggest that customers check their normal workflows. We can provide training after releases to ensure that users make the best use of the upgraded software and ensure they know how any changes might effect them.	Noted.

Subscription options			
6.75	What is the minimum level of commitment must the customer sign up to, e.g. 36 months?	12 months	Noted.
6.76	Where online payment is used, what type of security is used to protect sensitive information?	Altia uses Stripe to process credit card payment, who is a leading online transaction provider.	Noted.
6.77	Where online subscription / payment is used, is an invoice provided to the customer and, if so, in what format?	Yes Altia provides an invoice post payment processing.	Noted.
6.78	When subscriptions need to be renewed, what advance notice is provided and what is the time limit for renewal?	Customers are contacted 90 days before subscription renewal for both cloud and onpremise contracts.	Noted.
6.79	Is there a procedure for late renewal and is there a time limit after which subscriptions cannot be renewed?	Subscriptions must be renewed before the renewal data.	Noted.
6.80	How soon after creating or renewing a subscription (if applicable) can the system / service be used?	Typically within 5 working days.	Noted.
6.81	What notifications / confirmations are provided to the customer regarding subscriptions and payments?	Email confirmation is provided.	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?	For cloud customers data must be extracted prior to contract end.	Noted.
6.83	At the end of the contract term, how long does a customer have to obtain a copy of their data from you?	For cloud customers data must be extracted prior to contract end.	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?	Data and environments is deleted within the Azure portal shortly after contract completion. Azure then uses NIST SP-800-88 standard when the physical destruction of devices takes place.	Noted.
6.85	What is your processes regarding disposal of end-of-life and failed hardware devices that were used to operate your service?	This is handled by Microsoft Azure.	Noted.
SaaS/Hosted reporting			
6.86	Are reports produced from the same software as the financial applications or is separate reporting software used?	Reports are produced in product.	Confirmed.
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?	For on-premise customers, yes the Toolkit application and Toolbar Excel addin would both need installing.	Confirmed.
6.88	What browser versions are support: - On desktop/laptop (PC, Mac, Linux)? - On Tablets? - On mobiles?	Any browser that supports Azure Virtual Desktop. It is not supported on Mobiles or Tablets.	Confirmed.
6.89	Is access to the reporting facilities and data controlled by the same procedures as access to the main application?	Yes	Confirmed.
6.90	If it's different, explain the user access control facilities available to ensure information is only viewed by users with appropriate authority?	NA	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?	All export files types supported from Excel, including PDF, xlsx, csv etc.	Confirmed.

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?	For on preimise on a users computer, for cloud customers within the Azure Virtual Desktop.	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?	Documents are not viewed in the browser.	Confirmed.
6.94	Are communications between the browser and the server encrypted for any report related communications?	Yes using TLS 1.2+.	Noted.
6.95	If reports are produced dynamically each time the user views them can historical reports be reproduced at any time?	Yes, based on the source data provided.	Confirmed.
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?	Reports are only viewable through the application unless exported.	Noted.
6.97	Can report data be reliably copied and pasted direct from browser viewable reports to an MS Excel spreadsheet retaining any table layout?	Yes, mainly it is already within the Excel spreadsheet.	Noted.
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?	Report generation will not stop half way through without an error alert.	Noted.

Ref	Requirement	Response	Reviewer Comments
7	**DIGITAL BANK STATEMENT ANALYSIS**		
Global setup			
7.01	Does the digital bank analysis software operate on a client-by-client or engagement basis when setting up and managing analyses? If not, please explain how a user initiates and structures a new bank analysis within the system, including how it is organised and attributed.	No. Altia FIT (Financial Investigation Toolkit) is a Microsoft Excel add-in, not a case management platform. There is no client or engagement record structure within the application itself. Files are organised at the OS/file system level by the user. Each processed bank statement results in a standalone Excel workbook. Multiple accounts can be merged into a single workbook for cross-account analysis using the Analysis Toolbar's Merge Account function.	Confirmed.
7.02	If the software operates on a client-by-client or engagement basis, does it capture key details such as client/engagement information and currency? If so, can multiple currencies be supported, and which currencies are available?	The Toolkit captures account name, account number, sort code, and opening balance at the point of processing. There is no formal client or engagement field. Currency is handled via configurable credit/debit identifiers during processing. The Currency Converter Tool in the Analysis Toolbar supports multiple currencies: Basic Mode converts to AUD, CAD and EUR; Subscription Mode supports all currencies.	Noted.
7.03	Does the system integrate to accounting/financial packages? If so, please list which ones are supported and explain the method of integration (e.g. dedicated connector, webservices, CSV file transfer, etc):	FIT integrates with Altia Insight via the 'Export as Insight Import File' function, which produces a file suitable for import into Insight (subject to Insight version compatibility). No integrations with third-party accounting packages (e.g. Xero, Sage, QuickBooks) currently exist.	Noted.
7.04	Does the software directly integrate with on-line financial institutions [hereafter referred to as "Banks"]? If yes, please list the packages/services in the categories below and explain the method of integration (e.g. dedicated connector, webservices, etc): - Banks? - Building Societies? - Credit card providers/operators (e.g. Visa, MasterCard)? - Others, please specify? Additionally, please specify which UK Financial Institutions the software connects with and which it doesn't.	No. FIT does not have live connections to bank portals or open banking APIs. It processes electronic files (CSV, Excel, PDF) supplied directly by banks or exported by account holders, using bank-specific data loaders. There is no direct electronic request mechanism to banks. UK data loaders (electronic file and/or PDF formats) are available for: Barclays (Bank, Barclaycard, Barclaycard Commercial, Business Current Account, Premier Account, Barclaycard Historic PDF), HBOS, Lloyds (PDF), Monzo (PDF), Nationwide (PDF), NatWest, PayPal, Santander, Revolut (Account Statement), American Express UK, Scotia, First Bank (PDF), Bank of America, American Express US, Halifax (PDF, Excel), TSB (Mini Statement and Bank Statement), Starling, Co-Op, Metro Bank, SuitsMe (PDF, added v8.2.0), Republic Bank. Also supported: Clarien PDF (v8.2.0), Banco Ideal Business, Banco Smart Checking. Australian institutions: NAB, BankSA, CBA, Teachers Mutual Bank, Westpac, ING. Peruvian institutions: BCP, BBVA Continental, Interbank, GNB. Australian PDF.	Noted.
7.04 cont.		Amex Platinum (AUS), Amex Qantas Business Rewards (AUS) (both v8.2.0). Additional banks can be supported on request — Altia will work with customers to add new electronic formats.	
7.05	Does the system hold a master list of the addresses and web-access details (the Open Banking link) for the most common Financial Institutions, and enable these to be selected on-screen without manual input of the details?	No. This is not applicable as FIT does not use Open Banking or direct bank connections.	Noted.

Ref	Requirement	Response	Reviewer Comments
7.06	If a third-party provides the connection to the Bank please provide details of the provider.	Not applicable. No live bank connections exist.	Noted.
7.07	Does the system make use of global lists, e.g. Banks, Postcodes, VAT codes? If so, specify what is provided.	Not documented. Statement Profiles and Pattern Manager Rule Files can be shared across users via import/export, providing a de facto shared configuration library, but there is no built-in global reference data list for postcodes or VAT codes.	Noted.
7.08	Does the system allow a user to use multiple devices, e.g. a desktop and a tablet?	FIT is a Windows desktop Excel add-in (Windows 10 or later, Microsoft Office 2013 or later, 64-bit compatible). It is not a browser-based or tablet-compatible application. It can be installed on multiple PCs under the per-seat or Network Licence Service (NLS) model. Citrix and thin-client server deployments require special agreement with Altia.	Noted.
7.09	Does the system provide the facility for off-line working, i.e. downloading engagements for analysis away from the office? If so, please explain how this operates.	Yes. Core processing functions (data ingestion, formatting, analysis) work fully offline. Internet connectivity is required only for: in-app help and hint sheets, version update checks, inflation data downloads, and currency conversion in Subscription Mode.	Noted.
7.10	Does the system provide a facility for auto-saving changes to an engagement during a user's editing session? If so: - Can the frequency of these auto-saves be manually set? - Can the user initiate a save manually? - Can a user roll back to a previous saved version?	FIT does not have a proprietary auto-save feature. Excel's native auto-save and auto-recovery functionality applies. The Toolkit provides a dedicated 'Save As' button on the ribbon for saving to Excel format, and a 'Reload' button to reload the original source file. No roll-back to previous saved versions is provided within FIT itself.	Confirmed.
7.11	Does the system provide inbuilt workflow functionality? If so, please explain how this operates.	No. FIT does not have workflow, task assignment, or approval routing functionality. It is a data processing and analysis tool.	Confirmed.
7.12	Does the system have an audit trail that includes details of: - Changes to standing data (global lists)? - Transactions received from banks? - Transactions uploaded from spreadsheets? - Transactions sent to/from accounting system(s)?	No dedicated audit trail is documented. FIT is a desktop Excel add-in and does not maintain server-side logs of user actions, transaction modifications, data changes, or imports. As a desktop tool, access control and activity logging are managed at the operating system or network level by the customer's own IT infrastructure.	Noted.
7.13	Does the system come with a library of standard analysis templates that can be applied to a new engagement? *[This is the grid or spreadsheet output that the platform uses to show/filter the resulting statement data.]*	Yes. Statement Profiles are pre-configured templates that define how different bank statement formats are processed (column mappings, date formats, error correction rules, multi-row transaction handling). These are applied when processing raw data. The Analysis Toolbar includes a library of standard Quick Reports and Pattern Manager Rule Files. Statement Profiles and Rule Files can be shared between users via import/export.	Confirmed.

Ref	Requirement	Response	Reviewer Comments
7.14	If so, what do these cover? For example: - Insolvency compliance? - Audit validation/analysis? - Other, please specify?	Statement Profiles: cover all supported bank formats (UK, Australian, Peruvian institutions as listed above), OCR output formats, and general tabular data. Quick Reports include: Description Groupings (fuzzy matching), Cross Account Transfers, Credit Turnover, Debit Turnover, Benford's Analysis, Narrative Groupings, Bank Account Movement, Recurring Transactions, Sum of Monthly Transactions, End of Month Balance, Debit by Type, Credit by Type, Transaction Period Report, Electronic Account Transfer Report. Templates are not pre-categorised for specific use cases such as insolvency compliance or audit validation - categorisation is managed by the user through custom Rule Files and profiles.	Noted.
7.15	If so, does the analysis template include: - Selections of tests and associated parameters? - Result filters? - Risk indicators and associated limits? - Other settings, please specify?	Pattern Manager Rule Files define matching criteria (text, numeric threshold, date range, regular expression, item from list). Rule Files can flag transactions meeting specific criteria (e.g. values >= £10,000) and output results to new columns. Users can define their own risk thresholds. No pre-built risk scoring or weighting framework is included out of the box, but the Pattern Manager's rule engine allows users to construct equivalent logic. Benford's Law analysis is available as a standard Quick Report.	Confirmed.

Ref	Requirement	Response	Reviewer Comments
User setup			
7.16	Does the system provide a permissions matrix so that rights can be set at user and group level?	No. FIT is a per-seat desktop application. Access control is not managed within the product - it relies on the customer's OS, Active Directory, and file system permissions. There are no application-level user accounts, roles, or groups.	Noted.
7.17	Does this apply to: - Specific areas of functionality? - The link with Banks? - Specific clients? - Selection of the analysis template? - Manually adding/editing transactions? - Other, please specify?	N/A	N/A
7.18	Is it possible to define delegated access?	Not applicable as a desktop tool. These controls would be managed externally via OS/network permissions.	Confirmed.
7.19	Can multi-level authorisations be set?	No	Noted.
7.20	Are there restrictions on more than one user working on the same [single] client at the same time?	No	Noted.
7.21	Are there restrictions on one user working on multiple clients at the same time?	Not applicable within the application. Simultaneous editing of the same Excel file would be subject to standard Excel file locking behaviour.	Noted.
Client/engagement (statement analysis) setup			
7.22	Does the system provide for the setup and maintenance of a client/engagement details?	No. FIT does not have a client management module. Client and engagement organisation is managed at the file system level by the user.	Noted.
7.23	Can a client hierarchy be entered so that clients with multiple offices or legal entities can be processed?	Not applicable - no client management functionality.	Noted.
7.24	Can multiple clients be linked to one head-office address?	Not applicable - no client management functionality.	Noted.
7.25	Does the system hold details of a client company's directors [for use in the subsequent analysis]?	Not applicable - no client management functionality.	Noted.
7.26	Does the system allow the entry of supplementary information, e.g. Notes?	Yes. FIT allows users to insert supplementary transaction notes or atatchments. Users can assign categories for each attachment, edit those categories and select types of documents that can be attached.	Confirmed.
7.27	Does the system incorporate dashboard functionality such that the following information is presented to the user on their "home page" when they login to the system, showing: - All active engagements that the user is involved in? - Progress/completion of each engagement? - Any actions outstanding?	No. FIT opens directly within Excel. There is no dashboard, home page, or engagement progress view.	Confirmed.
7.28	Does the system allow all engagement files for a client to be: - Shown as a list on-screen? - The details viewed on-screen? - The details to be printed out?	Not applicable - no for management functionality.	Noted - N/A.
7.29	Does the system provide a straightforward way to search for engagements, with search parameters such as: client, engagement, year, date-range?	Not applicable - no engagement management functionality. File search is handled by the OS.	Noted - N/A.
7.30	Does the system provide the ability to delete engagements/audits, subject to the permissions matrix? If so, is this noted in the audit log?	Not applicable	Noted - N/A.

Ref	Requirement	Response	Reviewer Comments
Obtaining bank transactions			
Authorised access:			
7.31	Can multiple Banks be to linked to a client/engagement?	Multiple bank accounts (from any institutions) can be merged into a single master spreadsheet using the Analysis Toolbar's Merge Account function. This interleaves transactions by date across all accounts and enables cross-account analysis. There is no formal 'client' structure to link accounts to - the merged workbook is the unit of analysis.	Noted.
7.32	Can multiple sets of bank account details be held against each Bank [for each client]?	Yes	Noted.
7.33	Does the system hold details of the client contacts who can provide authority for the system to access each bank account? - If yes, what details are held? (e.g. name, email, mobile)	No. There is no client contact or authorisation management functionality.	Noted.
7.34	Can the user make an electronic request to their client for them to provide access to their bank accounts? If yes, can this be: - Via a personalised link in an email? - Via a personalised link in a text message? - Display of a personalised link that can be copied/pasted into another application for sending to the client? - Other, please specify?	No. FIT does not have open banking connectivity or an electronic client authorisation workflow.	Noted.
7.35	If a URL is provided to the client: - Is this a secure web-address? - Does the link expire? If so, after how long?	Not Applicable	N/A
Data ingestion (Downloading transactions):			
7.36	Does the system have the facility, where authorised (as above) to make electronic requests of a client's electronic banking portal in order to return lists of transactions covering specific time-periods?	Yes. Four ingestion routes are available: Scan and OCR, General Dataloader, Financial Dataloader, Tab deliminated text file.	Noted.
7.37	How does the user do this within the system? E.g. - By adding a new request against a client; - Selecting the bank and pre-authorised account; and - Entering a transaction date range.	Yes - via the separate Altia OCR Tool. Users scan paper statements; the OCR Tool extracts transaction data and exports a file, which the Investigation Toolkit then processes into the standard Excel format. Cheque scanning and OCR is also supported.	Noted.
7.38	Does the system automatically link to the selected bank, post the request and accept the returned transaction list from the Bank? Alternatively, is another process followed?	Yes - automatic data loaders convert PDF statements from supported banks (e.g. Barclaycard Historic PDF, Lloyds PDF, Nationwide PDF, Monzo PDF, First Bank PDF, SuitsMe PDF, Clarien PDF, Halifax PDF, Amex AUS PDFs, and others) directly into the standardised format.	Confirmed.
7.39	Is the request saved in a list of submitted requests together with the result of the request (accepted, rejected, failed, etc) and the resulting list of transactions.	Yes	Noted.
7.40	Are the transactions returned from a Bank saved in a standard format within the system, i.e. does the system have a download template for each Bank that enables data to be downloaded/converted into a single consistent format?	There is no single default - the appropriate method depends on what format the statement is available in. For supported banks with electronic export files, the dataloader route is recommended as it requires minimal manual input. The OCR route is used for paper or non-natively-supported statements.	Noted.

Ref	Requirement	Response	Reviewer Comments
Alternative ingestion methods:			
7.41	Does the system provide alternative methods to ingest bank statement information? If so, please detail these, including: - Scanning / OCR of hard copy statements? - Conversion of electronic statements in PDF format? - Conversion of electronic statements in Excel format? - Other, please list all methods available:	Yes - structured export files from supported banks (e.g. Barclays CSV/export, NatWest, Lloyds, Revolut, etc.) are processed via dedicated data loaders that automatically strip extraneous data and convert to the standardised format.	Confirmed.
7.42	Does the system have an inbuilt statement "format" for each Bank that enables data to be captured and converted into a single consistent format (as per for the direct electronic download described above)?	Yes. Statement Profiles define the mapping from each source format to the standardised Altia spreadsheet format (date, description, credit, debit, balance columns). Profiles are selectable at processing time and can be saved, shared, and modified.	Noted.
7.43	Please explain which ingestion methods are provided by the platform and which is the default option.	Altia Scan and OCR Tool, Dataloaders, Tab Deliminated File, Excel workbook. The default ingestion method is via the Scan and OCR tool.	Noted.
OCR ingestion:			
7.44	Does the OCR functionality support recognition of non-standard text formats (e.g. handwritten entries), and if so, what are the limitations and expected accuracy levels?	The OCR Tool is designed for printed bank statements. Handwritten entry support is not documented. Common OCR misrecognition errors (e.g. '8' for 'B', '1' for 'l', date format errors) are corrected via configurable automated rules and manual correction workflows. Page image links allow users to navigate directly to source pages for error correction.	Confirmed.
7.45	What languages are supported by the OCR functionality, and are there any limitations in accuracy or feature availability across different languages?	English Afrikaans Albanian Arabic Bulgarian Byelorussian Catalan Chinese (Simplified) Chinese (Traditional) Hong Kong Supplementary Croatian Czech Danish Dutch Estonian Finnish French Gaelic (Irish) Gaelic (Scottish) German Greek Hebrew Hungarian Icelandic Italian Japanese Korean	Confirmed.

Ref	Requirement	Response	Reviewer Comments
7.45 cont.		Latvian Lithuanian Macedonian Moldavian Norwegian Polish Portuguese Romanian Russian Serbian Slovakian Slovenian Spanish Swedish Thai Turkish Ukrainian Welsh Xhosa Zulu	
7.46	Please specify the data fields captured during document ingestion (e.g. account numbers, sort codes, transaction metadata), and whether this varies by ingestion method (e.g. OCR vs API vs file upload).	Standard FIT fields: Date, Description, Credit, Debit, Statement Balance (plus calculated running Balance). Additional: Account Name, Account Number, Sort Code, Opening Balance, Opening Date, Transaction Type column (where present in source). Page image reference links are retained if the OCR 'Include Page References' option is used. Field availability varies by ingestion method - electronic data loaders auto-populate most fields; OCR and general data routes require manual column mapping via Statement Profile.	Confirmed.
7.47	Where the system extracts tabular data (e.g. via OCR or structured parsing), can users manually adjust column alignment, field mappings, or extracted values? If so, how are such amendments controlled and logged?	Yes - column mappings, date formats, and processing options are set on the processing form and can be saved as Statement Profiles. Individual transaction values can be manually edited in the spreadsheet (e.g. correct OCR errors, modify dates, adjust credits/debits). These manual edits are not logged within FIT itself - there is no built-in audit log for transaction amendments.	Confirmed.
Initial validation:			
7.48	Can a user make changes to the transactions downloaded (subject to the permissions matrix)? If so, is this recorded in the audit log?	Yes - users can insert blank transactions, edit description text, modify transaction dates, swap credits/debits, move values between columns, and adjust decimal positions. These changes are not recorded in an audit log within FIT. Changes are permanent within the Excel workbook; previous states are not tracked by the application (though Excel's own undo history applies within a session).	Confirmed.

Ref	Requirement	Response	Reviewer Comments
7.49	Does the system undertake an initial set of validation checks to ensure that the data has imported correctly? If so does this include tests of: - Data types in particular fields? - Data ranges? - Field values ("sensible" upper and lower limits)? - Corrupted data?	Yes. Validation checks include: data type validation (dates, decimal values), balance reconciliation (calculated running balance vs. statement balance), date sequence checking (out-of-order dates flagged), and detection of format issues in the source file. Errors are highlighted in the spreadsheet and a 'Select Errors' navigation tool allows the user to step through each error. If non-correctable errors are detected, the user is alerted and shown the first error. Processing can be re-run after correction.	Confirmed.
7.50	Does the system also check where in the transaction (statement line): - The value is zero? - There are round amounts? - Multiple transactions are to the same payee? - Transactions are in a specific currency? - Other, please specify?	Round amounts and same-payee grouping can be identified post-ingestion using Pattern Manager rules and Quick Reports (e.g. Description Groupings, Recurring Transactions). Zero-value and currency-specific filtering can be applied via Excel's native filter functionality or Pattern Manager rules.	Noted.
7.51	If the system provides an initial check for gaps in the data please explain the logic for this?	Date sequence checking detects out-of-order transactions, which may indicate missing pages. Balance mismatch detection (calculated vs. statement balance) also provides an indirect indicator of missing data. There is no explicit 'gap detection' report - gaps are typically identified by the user reviewing the date range and balance continuity.	Noted.
7.52	If the system provides an initial check for duplications in the data please explain the logic for this?	Duplicate or missing transaction data in the source file is listed as a known cause of processing errors. The system detects these during processing and reports them. The documentation does not describe an explicit standalone duplication report.	Noted.
7.53	Please explain what the system does in the event that data fails the initial validation? e.g. The logs/report(s) provided, what happens to the import (rejected/part-rejected/etc).	Errors are highlighted in the spreadsheet (conditional formatting). The Select Errors button navigates the user through each error in sequence. On the second processing run, higher-level errors (balance mismatches, date sequence issues) are reported. The user must manually correct errors and reprocess. Imports are not rejected wholesale - partial processing occurs and the user corrects incrementally.	Noted.

Ref	Requirement	Response	Reviewer Comments
Data cleansing:			
7.54	Does the system undertake a series of cleansing activities on the transaction data after it has been downloaded?	Yes.	Noted.
7.55	If so, please explain the activities included, such as: - Removal of headers/footer/blank-lines for non-electronic-banking imports? - Removal of comment lines? - Removal of lines with no transaction value? - Other?	Cleansing activities include: automated removal of non-transaction rows (headers, footers, balance brought forward rows, blank lines) via Statement Profile settings; automated OCR error correction (configurable rules for common character substitutions in date and currency fields); multi-row transaction handling (correctly assembles transactions split across multiple source lines); removal of extra spaces from description column; debit/credit identifier normalisation; decimal separator correction.	Noted.
7.56	Please describe the redaction functionality within the software, including whether redactions are permanent once applied and whether any audit trail or controlled reversal functionality is available.	The Redact Statement tool (in the Analysis Toolbar) allows redaction of Account Name, Account Number, Sort Code, and Description fields. Options include: Redact Trailing, Redact Leading, or Redact All characters; configurable redaction character (default '*'); fixed-length or character-by-character redaction; fuzzy-matching for description content; import/export of redaction lists. The documentation does not explicitly confirm whether redactions are permanent or reversible once applied. This should be confirmed with the development team before submission.	Confirmed.
<u>Analysis and review</u>			
7.57	Once the statement data has been ingested, validated and transformed to the system's default format, does the system undertake a series of analysis tasks on the data?	Yes — via the Analysis Toolbar (a separate but related Excel add-in). Analysis capabilities include:	Confirmed.
7.58	If so, please provide a list of the main categories of tasks undertaken?	Pattern Manager (rule-based flagging and classification); Transaction Matching (automated and manual money flow identification between accounts); Quick Reports suite; Easy Pivot Table; Merge Account (multi-account consolidation); Currency Conversion; Inflation Calculator; Description Groupings (fuzzy matching); Benford's Analysis; Power BI integration.	Confirmed.
7.59	Does the system undertake specific analysis on the names of individuals referenced in transactions? If so, please explain what is undertaken?	Yes. Pattern Manager can pick out names from transactions and export them in a new column. Users can then use a narrative groupings report to generate transactions by account holder reports. Users can also generate description groupings report which will generate 3 follow up reports of transactions that are similar which will pick up names from transactions.	Confirmed.

Ref	Requirement	Response	Reviewer Comments
7.60	If yes, does this include undertaking a analysis that matches the payee with the previously identified directors of the client company?	The Pattern Manager can search the Description column (and other columns) for named individuals or entities using text matching, regular expressions, or item-from-list rules. Description Groupings uses fuzzy matching to group similar payee names. The Electronic Account Transfer Report extracts account numbers embedded in transaction descriptions.	Noted.
7.61	If yes, does this include an API link to Companies House to verify the directors previously identified?	Yes	Noted.
7.62	Is it possible for the system to also undertake a lookup (on demand) at Companies House for any selected company in the list of creditors/debtors? Is do, is there an extra charge for this?	Yes - no extra charge for this	Noted.

Ref	Requirement	Response	Reviewer Comments
Resulting analysis:			
7.63	How does the system present the analysed statement data to the user, e.g. in a grid that can be manipulated within the system or via a formatted spreadsheet?	All output is presented within Microsoft Excel. The standardised workbook is the primary output, with additional worksheets generated by Quick Reports (charts, summaries, pivot tables), the Matched Transactions worksheet, and diagram worksheets. Money Transfer and Money Match diagrams are interactive within the Altia form and can be saved as JPG images or embedded in Excel worksheets. Power BI integration is available for further visualisation.	Confirmed.
7.64	Is the analysis file produced by the system presented in the list of client engagements against the associated client/engagement? If not, how does the user access it?	No - there is no client/engagement list. The user accesses output files via the OS file system or directly within Excel.	Confirmed.
7.65	If the analysis output file is provided in spreadsheet format, what formats are supported? - Excel (XLSX, XLS, XLSM)? - Lotus (.123, wk?)? - Mac Numbers? - OpenDoc spreadsheet (Ods)? - Other (please specify)	Primary output: Microsoft Excel (.xlsx). Additional: Export as Values Only Spreadsheet (.xlsx, formulas stripped); Export as Insight Import File; diagram save as JPG; Power BI data connection. Excel's native export functionality also allows saving as CSV, PDF, and other formats from within Excel.	Noted.
7.66	If a spreadsheet is used must the user enable macros in order to gain the full functionality of the analysis output spreadsheet?	No. FIT is an Excel Add-in installed via MSI, not a macro-based solution. No macros need to be enabled.	Noted.
7.67	Are there multiple levels to the grid / spreadsheet tabs, representing each of the analysis areas in the selected analysis template?	Yes. The standard workbook has a main transaction sheet. Quick Reports and Transaction Matching generate additional named worksheets (e.g. Description Groupings Summary, Description Groupings Detail, Matched Transactions, Balance Over Time, Account Report, etc.). Each report generates its own worksheet(s).	Confirmed.
7.68	Do the levels/tabs cover each of: - Transactions (the items that were on the statement)? - Entities (distinct payees found)? - Accounts (sort codes and account numbers in the data)? - Outlier-transactions (to then sort by largest/smallest)? - Round amounts (ditto)? - Other(s)? Please describe what is provided in the standard template(s).	Standard workbook: all transactions with date, description, credit, debit, balance, account name, type. Quick Reports provide: Description Groupings (payee analysis with fuzzy matching), Cross Account Transfers, Credit/Debit Turnover, Bank Account Movement, Recurring Transactions, Sum of Monthly Transactions, End of Month Balance, Debit/Credit by Type, Transaction Period Report (day of week/month/year breakdown), Electronic Account Transfer Report, Benford's Analysis, Narrative Groupings. Account Report summarises merged accounts with transaction counts and largest values.	Confirmed.

Ref	Requirement	Response	Reviewer Comments
7.69	For each level/tab is the user able to manipulate the grids of transactions, in order to : - Filter? - Sort (ascending and descending)? - Other (please specify)?	Yes. Filter: Excel's native filter functionality is available via the Altia Filter button (all columns or selected range). Sort: Sort By Date function (ascending/descending, with options to preserve or rebuild index). Custom Views (selective formatting). Find and Replace. Direct cell editing for manual amendments.	Confirmed.
7.70	Is the user able to: - View the data? - Filter it? - Manipulate transactions (i.e. edit statement line details? - Other?	Yes	Confirmed.
7.71	Does the system enable the analysis output data to be shown graphically? If so, can the user amend: - The graph type? - The format of the graphs? - The data ranges shown on the graphs? - Other, please specify?	Yes. Quick Reports generate charts (e.g. Balance Over Time, Recurring Transaction Totals, Day of Week Breakdown, Monthly Totals). Easy Pivot Table includes optional graph generation. Money Transfer and Money Match diagrams are interactive network diagrams showing money flow between accounts. Accounts can be colour-coded across diagrams and reports. Diagram format options: zoom, filter by minimum transfer amount, change layout, export as JPG. Power BI integration extends visualisation options further.	Noted.
7.72	Can a user add additional grid levels / spreadsheet pages and create additional data extracts/filters on these?	Yes	Confirmed.
7.73	Can multiple versions of the grid/spreadsheet be saved that incorporate different filters/data-sets?	Yes	Noted.
7.74	Can previously saved grids/spreadsheets to re-opened, amended, and subsequently re-saved?	Yes	Confirmed.
7.75	Can additional [manually created] tests be saved into the standard analysis template? If so, can multiple versions be created ?	Yes. Easy Pivot Table reports can be saved as named Quick Reports for reuse. Pattern Manager Rule Files add custom columns to the transaction sheet. Multiple workbook versions can be saved by the user. Statement Profiles and Rule Files can be shared across users.	Confirmed.
7.76	Can a set of risk/potential-fraud scores and/or weightings be applied to each of the tests? If so, explain what is available and how these are applied?	Not as a pre-built feature. Pattern Manager rules can output text flags or values to custom columns, allowing manual scoring to be implemented by the user. No automated risk scoring engine is built in.	Noted.
7.77	Does the system apply any machine learning to the tests being run? If so, please provide details explaining how this operates, e.g. using data from similar previous analyses undertaken as part of the basis for comparison.	Description Groupings uses algorithmic fuzzy matching to group similar transaction descriptions. Benford's Analysis is a statistical technique. No ML-based pattern recognition, predictive scoring, or training on historical data is described.	Noted.

Ref	Requirement	Response	Reviewer Comments
Reporting			
7.78	Does the system provide a series of inbuilt reports that show for example: - A list of clients? - The associated Bank account details? - The link/authorisation status? - The date last accessed? - Other? If so, describe the reports available.	No system-level reports of this type exist - there is no client management module. Within a workbook, the Account Report Quick Report provides a summary of merged accounts with transaction counts and key metrics. The Attachments Summary Report lists all attachments in the workbook.	Noted.
7.79	Does the system enable filtered lists of transactions (that were analysed in the in-system grid or formatted spreadsheet) to be printed or exported from the platform?	Yes. Excel's native export functions allow any worksheet (including filtered views) to be exported to XLSX, CSV, PDF, or other formats. Export as Values Only Spreadsheet removes formulas. No dedicated 'export report' dialog exists within FIT beyond what Excel natively provides.	Confirmed.
7.80	Can these reports be filtered by: - Date range? - Payee? - Other, please specify?	Yes - Altia filter, Pattern Manager, and Quick Report options (date range, account selection, fuzziness) support filtering by date range, payee/description, and account. Most Quick Reports prompt for account selection and date/period options.	Confirmed.
7.81	Are all reports adequately titled and dated? e.g. report name, client name, pages, numbers etc.	Quick Reports generate worksheets with titles reflecting the report type. Totals are provided where applicable (e.g. Credit/Debit Turnover, Cross Account Transfers). Formal document-style page headers, client names, and page numbers are not automatically applied — these would be added manually or via Excel page setup.	Confirmed.
7.82	Do the reports provide totals where applicable?	Yes	Confirmed.
7.83	Does the system allow the layout of reports to be customised: - Font? - Paragraph style? - Page format? - Watermark, e.g. "Draft"? - Company logo/graphic? - Other, please specify	Not within FIT itself. Excel's native page setup, header/footer, and formatting tools can be used for this purpose.	Confirmed.
7.84	Can reports be output directly to other formats e.g. Excel, CSV, txt, XML, PDF etc. for any period of time required? - If so, please state the formats supported.	Via Excel's native Save/Export: XLSX, CSV, PDF, and other Excel-supported formats. FIT also provides Export as Values Only (.xlsx) and Export as Insight Import File. Diagrams can be exported as JPG.	Confirmed.
Future enhancements			
7.85	When new features or enhancements are developed in response to customer feedback, are these deployed universally across all customers or selectively to specific clients? Please describe your release strategy.	Updates are released as new software versions deployed universally to all customers. An in-app 'Check for Updates' function notifies users when a new version is available. New features and bug fixes are included in release notes distributed with each version. Based on version history, releases occur approximately quarterly.	Noted.

Ref	Requirement	Response	Reviewer Comments
7.86	Please outline the confirmed product development roadmap over the next three years, including key functional enhancements, expected delivery timelines, and any dependencies or constraints.	A formal three-year roadmap is not included in the publicly available user guide documentation. Currently we are expanding the range of dataloders available for more banks, an invoice reconciliation tool and a companies house tool for Canada and Australia. Please refer to Altia's product team for the current roadmap.	Noted.