

Ref	Requirement		
	HEADER		
	ICAEW Technical Accreditation Scheme Legal & Research Software Evaluation		
	GenIA-L		
			
	August 2026		
	© 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: (to follow deep dive demonstration if deemed appropriate)		
7	Legal & Information Research		

Ref	Requirement	Response	Reviewer Comments
1.	<u>INTRODUCTION AND PROLOGUE</u>		
Introduction			
1.01	The suitability of software for each particular user will always be dependent upon that user's individual requirements. These requirements should therefore always be fully considered before software is acquired. The quality of the software developers or suppliers should also be considered at the onset.		
1.02	Fundamentally, good software should: 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:	GenIA-L is Indicator's proprietary AI assistant, developed by our R&D team in Madrid. We are part of the leading legal and tax knowledge business, Lefebvre, based in Paris.	

Ref	Requirement	Response	Reviewer Comments
1.09	Supplier background:	Indicator produces compliance content and research tools for SME audiences across tax, HR, health and safety, company law, payroll, and environmental topics. Its content is developed by subject-matter specialists and is designed to give professionals clear, authoritative, evidence-backed guidance. GenIA-L is based exclusively on the documentation holdings of the group's local publishing houses, ensuring users receive reliable answers grounded in verified and up-to-date sources. The platform is built on the principle of responsible AI — with traceability, zero data retention, and EU hosting — designed to support professionals without replacing their expertise. Lefebvre GroupLefebvre Group Indicator has already secured accreditation from the Institute of Certified Bookkeepers (ICB) for GenIA-L, following an independent review by a panel of practising ICB bookkeepers, who were particularly impressed by GenIA-L as a tool for helping members work more efficiently.	
1.10	Product background and suitability for the user:	GenIA-L is Indicator's conversational AI assistant, launched into the UK tax and accountancy market as an unprecedented tool designed specifically for tax advisors and accountants. It takes tax advisory into the digital age with machine learning capabilities, offering tailored advice through an intuitive chat interface, including the ability to upload contracts and spreadsheets for analysis and comparison. The case for GenIA-L in an accountancy context is strong and timely. According to Thomson Reuters' 2025 GenAI report, 89% of tax firm professionals believe GenAI can be applied to their work, and 71% say it should be — up from 52% in 2024. Enterprise-level adoption has also jumped, from 8% to 21% of firms in a single year. Thomson Reuters Tax What sets GenIA-L apart from general-purpose AI tools is the quality of its underpinning content. Indicator's AI assistant doesn't merely automate but innovates, giving tax professionals a significant edge in managing complex compliance obligations and delivering insightful advice to clients.	
1.10 cont.		Crucially, answers are drawn solely from Indicator's expert-authored content — not the open web — meaning accountants can trust what they receive. For ICAEW members specifically, GenIA-L supports the kind of work that defines modern accountancy practice: navigating complex tax questions quickly, comparing documents and identifying risk, and generating client-facing outputs with confidence.	
1.11	Add-on modules:	N/A	

Ref	Requirement	Response	Reviewer Comments
1.12	Typical implementation [size]:	GenIA-L is a cloud-based SaaS tool accessed via a browser — there's no on-premise installation, no IT infrastructure requirement, and no technical knowledge needed to use it. Users simply ask questions in plain English through a simple chat interface, or upload documents for analysis. This low-friction onboarding makes it accessible to firms of all sizes without specialist support.	
1.13	Vertical applications:	While GenIA-L spans multiple verticals (including company law, payroll, HR and H&S), the tax and accountancy vertical is the primary focus for ICAEW members — encompassing income tax, corporation tax, VAT, capital gains, and financial reporting. The multi-vertical architecture also means ICAEW members advising SME clients get ancillary value across HR and company law without needing separate tools.	
1.14	Server platform and database:	GenIA-L is built on enterprise-grade, GDPR-compliant, EU-hosted infrastructure, with a zero data retention policy — user data is not stored or reused. Indicator The platform was developed by Lefebvre's R&D team and, at launch, was integrated into the NEO and QMemento legal databases in Spain — these are Lefebvre's proprietary content repositories. The UK equivalent draws on Indicator's own curated content library. GenIA-L uses a proprietary algorithm developed by Lefebvre's R&D team — so it is not simply a wrapper on a generic LLM. The underlying AI engine and retrieval architecture are group-developed.	
1.15	Client specification required:	Current version of Chrome, Edge, Firefox, or Safari Stable broadband connection No specific OS requirement (Windows, macOS, iOS, Android all viable) No minimum hardware specification beyond what runs a modern browser Document upload functionality (for contract/spreadsheet analysis) will require sufficient connection speed for file transfer	
1.16	Partner network:	N/A	

Ref	Requirement		
2.	ISSUES AND CONCLUSION		
Highlighted issues			
2.01	There are a number of limitations in the product, which while not adversely impacting upon this evaluation may be of importance to some organisations. It is important that any business contemplating the purchase of software reviews the functionality described and limitations therein against its detailed requirements. Attention is drawn in particular to the following areas where the product, on its own, may not be suitable for businesses with certain requirements:		
2.02	Findings for considerations by potential customers: (See vendor comments against the various questions).	Question reference	
2.03	The platform relies on curated professional content authored and maintained by the vendor. As updates to legal and regulatory content are subject to editorial review and publication processes, there may be a delay between changes taking effect and their availability within the platform. Where legislation, regulations or guidance include clear effective dates, this is unlikely to present a significant issue. However, where this is not the case, the vendor currently targets updates within one week of a change. Customers should consider this when using the software for time-sensitive research and review the publication and effective dates of the underlying source materials where relevant.	7.18	
2.04	The software is continually being enhanced, and the vendor has identified a number of planned developments on its future roadmap, which prospective customers should consider as part of their assessment: July 2026 – Excel file and spreadsheet analysis support released. 2026 – Expansion of the UK professional content corpus. 2026 – Vault, which is secure history and content-management capability. 2026 – Improvements to prompt processing, interpretation and response quality. 2026 – Enhanced retrieval, evaluation, monitoring and user functionality. By end 2026 – Increased document upload limits and improved processing of large, scanned and image-based documents. Q1-Q2 2027 – New platform with enhanced content search across additional Lefebvre content collections. Q1-Q2 2027 – User-profile personalisation and guided follow-up questions. Q1-Q2 2027 – Native voice-typing functionality and prompt library. Q1-Q2 2027 – Enhancements to navigation, content discovery and overall user experience.	7.42, 7.72	
2.05	Customer prompts, uploaded documents and generated outputs are not used to train, fine-tune or enrich either the vendor's models or third-party foundation models. Product improvements are informed only by explicit user feedback submitted through the platform's feedback mechanisms.	7.06	
2.06	The software incorporates a range of preventative and monitoring controls, including authentication and entitlement checks, source-grounding controls and responsible-use guidance, to restrict harmful or out-of-scope use. Organisations should reinforce these controls through their own AI Responsible Use Policy, governance framework and user training.	7.53	

Ref	Requirement		
2.07	Multi-factor authentication (MFA) is enforced for vendor technical administrators only. Customer administrators cannot currently enable or enforce MFA through the GenIA-L administration interface. Customers requiring mandatory MFA for all users should assess whether this can be enforced through their own identity provider and SSO configuration.	7.66, 7.67	
2.08	Customer administrators cannot currently configure password complexity requirements beyond the platform's baseline controls, and password history/reuse prevention is not currently implemented within GenIA-L-managed authentication. Customers requiring enhanced password controls should assess whether these can be enforced through their existing identity provider and SSO configuration.	7.72	
Evaluation conclusion			
2.09	For the specific use-cases in support of assisting accountancy firms to make effective use of Legal Information & Research software, for which the product is designed, the solution appears to meet this criteria. The platform includes a range of supporting capabilities designed to improve usability and adoption, including guidance, examples and onboarding support to help users formulate effective queries and generate structured outputs, as well as accessibility features such as screen reader support, keyboard navigation and text-resizing functionality. These features, while not exhaustive, contribute positively to the overall user experience and accessibility of the solution. Members should, however, remain aware of the limitations of the solution noted above and fully understand the role it can play in supporting, rather than replacing, the management of 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			
2.10	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.	<u>ACCESS AND SECURITY</u>		
Access control			
3.01	What security features are included to control access to the application?	Access to the application is strictly controlled through strong authentication mechanisms and fine-grained authorization based on the principle of least privilege (RBAC). Multi-Factor Authentication (MFA) is enforced for administrative access. All access requests are managed and secured via an API Gateway, ensuring token validation, request filtering, and protection against abuse. Direct access to the solution and underlying storage is strictly restricted. Administrative access is limited to named, individual secure accounts, with tightly controlled permissions to prevent unauthorized access and reduce internal security risks. Overall, these layered controls ensure that only authenticated and authorized users can access the application and its resources.	Noted
3.02	Can access to functions be managed via a permissions matrix so users can only see (in menus and other links) and access those areas they are authorised to access?	No need, there is only one profile.	Confirmed
3.03	Is this access to the application managed by:- - Individual user profiles? - User groups or job roles?	Individual user profile	Confirmed
3.04	Can a report be produced detailing all current users, their user groups if relevant, and their authority levels and/or access rights?	yes, a report can be produced on-demand of the customer's subscription administrator	Noted
3.05	If menus can be tailored does the system limit the display of menu options to those for which permission has been granted for each user?	The menu cannot be tailored	Confirmed
3.06	Does security allow for access to be limited to: - Read only? - Read/write? - Read/amend/delete?	Access management is based on the principle of least privilege. GenIA is accessed via a prompt-based interface (question/answer), where users do not have direct access to underlying data for reading, writing, or deletion. The underlying data (document corpus) is available in read-only mode. No modification or deletion rights are granted through the application interface. Access to the application code is restricted to the development team and managed separately under controlled access policies.	Noted
3.07	If data can be accessed by separate reporting facilities, such as ODBC or an external report writer, is the user access security control applied?	No, the solution does not provide separate reporting facilities such as ODBC connections or external reporting tools. Data is only accessible through the application via a question-and-answer interface.	Noted
3.08	Does the system security integrate with Microsoft's Active Directory or other tools that provide a single sign-on?	Yes. SSO integration with a client is possible when the client's Identity Provider (IdP) supports the protocol standards recommended by Lefebvre, namely: OpenID Connect or SAML.	Noted
3.09	Does the system provide multi-factor authentication (MFA)?	Only for technical administrator	Noted -Additional question asked in 7.66
Passwords and access logs			
3.10	Is access to the software controlled by password?	yes	Confirmed
3.11	Does each user have a separate log on (user ID)?	yes	Confirmed

Ref	Requirement	Response	Reviewer Comments
3.12	If there is no password facility please state how confidentiality and accessibility control is maintained within the software?	N/A	Noted
3.13	Are passwords masked for any user logging in?	Yes	Noted
3.14	Is password complexity available and enforced?	Yes Password policy requirements are as follows: Minimum length: 12 characters Complexity: must include uppercase letters, lowercase letters, alphanumeric characters, and special characters	Noted -Additional question asked in 7.68
3.15	How many previous passwords are retained / the password history?	This option is not currently implemented	Noted -Additional question asked in 7.69
3.16	Are passwords encrypted?	Yes, passwords are securely managed by Azure AD B2C. They are not stored in clear text and are protected using industry-standard encryption and hashing mechanisms	Noted
3.17	Are users automatically logged off after a pre-set idle time? - Can the time period be changed? - Can any information be viewed without being logged in, including after logging off, if so what information?	Yes, users are automatically logged off after a predefined session period. The encrypted chat session currently lasts 48 hours; however, it ends immediately if the user closes the browser. The session duration cannot be modified by the client. No information can be accessed without authentication. After logout or session termination, users must re-authenticate to access the application, and no data or functionality is available without being logged in.	Noted
Deletion of transactions			
3.18	Is it possible to delete a transaction?	if we consider a transaction as a query, no it's not possible. The main reason is that any information, besides the technical information (time, device, os, ...) is stored	Noted
3.19	If so, then how are deletions controlled by the system?	see 3.18	Noted
3.20	Are deleted transactions retained in the audit trail (see below) and denoted as such?	see 3.18 not possible to delete transactions	Noted
Audit trails			
3.21	Does the system have an audit trail (log) which records all changes to transactions in the system?	Logs are enabled to track user and administrator actions. Logs include: For users: Security events related to user logins. For internal/technical administrators: The same logs as for users, in addition to activity logs (read/write operations) across the different layers of the infrastructure.	Noted
3.22	Does this log also record any system error messages and/or any security violations?	Logs from these security components are also collected and analyzed to generate security alerts aligned with detection scenarios.	Noted
3.23	Is it possible to turn off or delete the audit trail?	No. The current architecture centralizes platform logs across all production environments, with retention periods defined to address security, operational, and compliance requirements (ISO, GDPR, incident traceability, transparency, and retention obligations). Appropriate security measures are implemented to ensure the confidentiality, integrity, and availability of these logs.	Noted

Ref	Requirement	Response	Reviewer Comments
3.24	Does the software allocate a system generated sequential unique reference number to each transaction in the audit log, date and time stamp it and record the user ID?	Yes, we identify every action with a single ID, so in case is needed we can track it	Noted
3.25	Are all master file changes recorded in the audit trail?	Yes, A logging system has been implemented to record all changes made to GenIA-L'Assistant files.	Noted
Compliance			
3.26	Does the system operate in a way that is compliant with data protection legislation including GDPR? How does the system facilitate this?	Yes, the system is designed to operate in compliance with data protection regulations, including GDPR. The solution is not intended to process personal data by design. However, recognizing that users may occasionally input personal data in prompts or uploaded documents, appropriate safeguards have been implemented. These include the absence of data retention (no storage of prompts or generated responses), no reuse of data for model training, and strict data minimization principles. The system follows privacy by design and by default, limiting processing to what is strictly necessary for real-time operation. Legal bases are identified where personal data could be introduced by users, and mechanisms are in place to support data subject rights where applicable. No automated decision-making producing legal or significant effects is performed. In addition, any involvement of third-party processors is governed by GDPR-compliant agreements.	Noted
3.26 cont.		Overall, the DPO has assessed that the solution includes sufficient safeguards to mitigate data protection risks and has validated its deployment, subject to maintaining these controls and reassessing in case of significant changes.	Noted
3.27	Describe your use of sub-processors if any?	IDP : Azure AD B2C LLM : OpenAI Hosting : AWS	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?	No, as the solution does not store customer data, backup and recovery mechanisms for customer data are not applicable. The system processes data only transiently (e.g. during prompt exchanges), and no persistent storage is maintained. Therefore, there is no requirement for data restoration procedures within the application	Noted
3.29	How often are backups taken and to what point can restores be done?	Not applicable	Noted

Ref	Requirement	Response	Reviewer Comments
3.30	How does the software facilitate recovery procedures in the event of software failure? (E.g. roll back to the last completed transaction).	In the event of a software failure, recovery procedures focus on service restoration rather than transaction rollback, as no persistent transactions are stored within the system. Recovery is managed at two levels: External services: recovery timelines depend on third-party providers Internal services: Standard issues: average recovery time under 15 minutes Major issues (e.g. database-related): average recovery time under 4 hours Infrastructure-as-Code and Kubernetes enable rapid reconstruction of the environment and duplication of infrastructure, ensuring efficient recovery in case of service disruption.	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?	Infrastructure-as-Code and Kubernetes enable rapid reconstruction of the environment and duplication of infrastructure, ensuring efficient recovery in case of service disruption. As the system does not rely on batch processing or persistent transactions, there is no need for rollback mechanisms. In the event of a failure, only the prompt exchange in progress may be impacted, with no requirement to reprocess previous interactions.	Noted
3.32	What features are available within the software to help track down processing problems?	The GenIA-L Assistant solution is integrated into IT monitoring tools to ensure full visibility across both infrastructure and application layers. Continuous monitoring of key performance indicators (e.g. service availability and resource usage) is implemented to detect and resolve issues promptly. An alerting system is configured to identify anomalies and trigger real-time notifications to technical teams when predefined thresholds are exceeded, enabling rapid intervention. In addition, real-time monitoring of usage and requests is performed, with controls such as request limitations (e.g. file size limits, payload size limits) applied to prevent misuse and ensure system stability.	Noted

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?	GenIA-L is not a menu-driven transactional accounting application. User input is made through a conversational prompt box and optional document upload controls. The interface guides users to ask questions in plain English or upload supported documents, and the platform applies authentication, request validation, file restrictions, processing controls and user-facing error messages rather than accounting menu workflows.	Confirmed
4.02	Are these menus user/role-specific?	No. The end-user interface is broadly consistent for authorised users, although access to content and functionality is governed by the customer subscription and user entitlement. Administrative functions are restricted to authorised administrators. GenIA-L does not expose accounting transaction menus or role-specific ledger workflows.	Noted
4.03	Can the creation or amendment of standing data (e.g. customer account details) be undertaken using menu options or dialogue boxes as opposed to requiring system configuration?	Not applicable to accounting standing data. GenIA-L does not maintain customer, supplier, nominal ledger, stock, currency or similar master records. User and subscription configuration is managed through controlled administrative processes and identity management; it is not a customer-facing accounting configuration screen.	Noted
4.04	Does the software provide input validation checks such as: - [account] code validation? - reasonableness limits? - validity checks?	Yes, for GenIA-L input types. Validation controls include authentication/session checks, prompt/payload length limits, supported file type and file size controls, file readability/structure checks and security filtering before processing. Accounting-specific checks such as nominal account code validation or VAT posting validation are not applicable because GenIA-L does not post or maintain accounting transactions.	Noted
4.05	What control features are within the software to ensure completeness and accuracy of data input?	Completeness is controlled at request level: a prompt or uploaded document must be fully received and pass validation before processing begins. Unsupported, incomplete, corrupted, password-protected or oversized files should be rejected with a user-facing message. Accuracy of generated answers is supported through retrieval from curated Indicator/Lefebvre content and source references; users remain responsible for professional review of outputs.	Noted - Additional question asked in 7.60
4.06	How does the software ensure uniqueness of the input transactions? (i.e. to avoid duplicate transactions)	GenIA-L does not create persistent accounting transactions, so duplicate transaction prevention is not applicable in the traditional sense. Each user request is processed as a discrete prompt/upload event and should be assigned a unique request or session identifier for traceability and troubleshooting. Duplicate prompts do not create duplicate accounting records.	Noted
4.07	Is data input by users validated by scripts or routines in the browser, or other client software, before transmission to the server?	Yes, to the extent applicable. The browser interface should enforce basic input constraints before submission, such as required input, supported file extensions, file size limits and upload status checks.	Noted

Ref	Requirement	Response	Reviewer Comments
4.08	Is data input by users validated by routines running on the server before data files are updated?	Yes. Server-side/API controls validate authentication, authorisation, request schema, payload limits, supported file types, file structure/readability and security filters before any AI processing. Because customer data is not written into a transactional database, the control objective is to prevent invalid or unsafe requests from being processed.	Noted
4.09	Does the above validation ensure that data entered in all input boxes: - Cannot be longer than a maximum length? - Cannot contain unaccepted characters such as semi-colons etc?	Yes. Maximum prompt/payload sizes and file size limits are enforced. Unsupported file types, malformed files, unsafe content and inputs outside accepted constraints are rejected or sanitised.	Noted
4.10	Are input errors highlighted?	Yes. Validation or processing errors are surfaced to the user through on-screen messages, for example unsupported file type, file too large, unreadable document, authentication/session issue or service error. Errors are also logged centrally for operational monitoring and support.	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?	Rejected inputs are not processed as successful requests. The user receives an on-screen message explaining the failure and, where appropriate, can correct the prompt or upload and resubmit. There is no temporary posting area or suspense account because GenIA-L does not post transactions.	Noted
4.12	Are responses to erroneous data input clear so that they do not lead to inappropriate actions?	Yes. Error messages should distinguish unsuccessful validation/processing from a completed answer and should direct the user to correct the input, retry or contact support.	Noted
4.13	Does the software have an automatic facility to correct/reverse/delete transactions?	No. GenIA-L does not create, post, correct, reverse or delete accounting transactions. A user can amend their prompt and submit a new request, but this does not reverse or correct a transaction in an accounting system.	Noted
4.14	If yes, are these logged in the audit trail?	N/A for accounting transaction correction because no such corrections are performed. Technical request metadata and platform events are logged in line with security and operational logging policies, subject to the zero-data-retention model for prompt/document content.	Noted
4.15	Are all data entries or file insertions and updates controlled to ensure that should part of a data entry fail the whole transaction fails?	Yes, at request level. A prompt or file upload is either accepted for processing after validation or rejected with an error. If part of an upload or request fails, GenIA-L should not treat the request as successfully completed and should notify the user. No partial accounting entries or persistent transaction updates are created.	Noted
4.16	Are messages provided to users clearly explaining whether the data entry or file upload has been processed successfully or not?	Yes. Successful requests result in an answer or generated output being displayed to the user. Failed prompts or uploads return an on-screen error or explanatory message.	Noted
Import and export of data			
4.17	Can files/attachments be uploaded and stored against any transaction?	Users can upload documents for analysis within the context of a prompt, but GenIA-L does not store files against accounting transactions because it is not a transactional accounting system. Uploaded files are processed transiently or in temporary secure processing storage and are not retained as a document repository under the zero-data-retention model.	Confirmed

Ref	Requirement	Response	Reviewer Comments
4.18	Is there an additional charge made for storage of uploaded files? - If yes, please indicate the cost.	No. GenIA-L does not provide persistent customer document storage for uploaded files; therefore no additional charge is made for storage of uploaded files.	Noted
4.19	Can data be imported into the system from multiple types of files, e.g. XLS, text, CSV?	GenIA-L supports document uploads for analysis, not transactional imports. For example PDF, DOCX, PPTX, JPG, . Unsupported, oversized, corrupted or unreadable files are rejected with a user-facing error.	Confirmed
4.20	Explain how the system validates imports into the system and what happens to any import which fails?	Uploaded files are validated for supported type, size, structure/readability and security before processing. Failed uploads are rejected and are not processed; the user is shown an error or retry message. No data is imported into a persistent accounting dataset.	
4.21	Are imported /interfaced transactions detailed in the audit trail? <i>[See also 3.27]</i>	GenIA-L does not import or interface accounting transactions. Upload/request events and technical metadata are logged for security and operational purposes. Prompt and document content should not be retained or reused under the zero-data-retention policy.	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?	GenIA-L outputs are displayed in the browser and can be exported and copied by the user.	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)?	N/A for accounting period-end or batch menus. GenIA-L processes each request independently. Internally, the system orchestrates validation, retrieval, generation and response steps in a controlled sequence, but there are no user-executed month-end or transaction-processing programs.	Noted
4.24	Does the software provide automatic recalculation, where appropriate, of data input? (e.g. VAT)	N/A for accounting recalculation such as VAT posting or ledger balances. GenIA-L may analyse figures in uploaded documents and generate explanatory outputs, but it does not maintain a recalculating accounting record. Users must professionally review any generated calculations.	Noted
4.25	Is a month/period-end routine required to be undertaken?	No. GenIA-L does not require month-end or period-end routines because it is a research and document-analysis assistant, not an accounting ledger.	Noted
4.26	Is it possible to delete accounts if the balance is Nil but transactions have been recorded against the code?	N/A. GenIA-L does not create or maintain accounts with balances or transaction history.	Noted
4.27	What is the size and format of reference numbers and descriptions within: - Ledgers? - Stock? - Currencies?	N/A for ledgers, stock and currencies. GenIA-L does not maintain those record types. Technical logs should use system-generated unique request/event identifiers and timestamps; user-facing answer traceability is provided through source references where available.	Noted
4.28	How does the software guard against/warn about duplicate account numbers on set up?	N/A. GenIA-L does not allow users to create accounting account numbers, so duplicate account number controls are not relevant.	Noted
4.29	How does the software enable the traceability [from, to and through the accounting records] of any source document or interfaced transaction?	GenIA-L provides traceability of answers through references and supporting source documents from the curated Indicator/Lefebvre content base. Where a user uploads a document, the generated answer is based on that document for the session/request. There is no traceability through accounting records because GenIA-L does not maintain accounting records or interfaced transactions.	Noted

Ref	Requirement	Response	Reviewer Comments
4.30	What drill down/around functionality is available within the software?	Users can follow references or supporting documents from GenIA-L answers back to the underlying source material, where sources are provided. This is the relevant drill-down mechanism for a research assistant. GenIA-L does not provide accounting ledger drill-down from balances to transactions.	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?	GenIA-L users do not maintain standing information tables. The curated content corpus and retrieval index are maintained centrally by Indicator/Lefebvre editorial and technical teams under internal content publication and release controls. Users do not amend these datasets through application parameters.	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)?	No traditional in-built report writer or third-party report writer is provided to customers. GenIA-L generates on-demand narrative answers, summaries, analyses and draft text in response to prompts, using curated source content and/or uploaded documents as context.	Confirmed
4.33	Is the report writer based on a standard SQL-type approach and is it flexible and easy to use?	N/A. GenIA-L does not expose a SQL-style report writer to users. Users interact through natural language prompts rather than SQL queries or report field selection.	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?	N/A. GenIA-L does not run a report generator over customer operational or financial datasets. It can analyse user-provided documents or spreadsheets within a prompt, but it does not combine stored financial and operational databases for reporting.	Noted
4.35	Is a comprehensive data dictionary provided to aid field selection?	N/A. There is no customer-facing report writer or data dictionary for report fields because GenIA-L does not expose structured report datasets to users.	Noted
4.36	Does the system provide a library of reports and templates which can be amended, saved and re-run?	No traditional library of saved reports/templates is provided unless prompt templates are available in the product. Users can create their own prompts and copy/reuse them outside the system.	Noted
4.37	Can users create their own reports? If so, what are the controls on users doing this?	Users can generate ad hoc draft outputs, summaries and analyses through prompts, but cannot create persistent report definitions that run against stored system datasets. Access to prompt functionality is controlled through authentication and subscription entitlement; outputs require user review before use.	Noted
4.38	Can users create saved searches/filters/queries?	No. GenIA-L searches are ad hoc natural-language requests; users can manually reuse previous prompt wording outside the system, but the platform does not provide persistent saved searches, filters or queries.	Noted
4.39	Can regular reports be added to user menus in the appropriate area of the system?	No. GenIA-L does not have a traditional report menu to which regular reports can be added. Users request outputs on demand through the conversational interface.	Noted
4.40	Does the system support the production of on demand (interactive) and scheduled batch reports?	GenIA-L supports on-demand interactive responses to user prompts. It does not currently support scheduled or batch report production.	Noted

Ref	Requirement	Response	Reviewer Comments
5.	USABILITY		
Ease of use			
5.01	Does the solution provide a multi-language user interface?	Yes, interface can be handle in English, French, Italian and Dutch.	Confirmed
5.02	Does the system allow for customisable branding and UI (e.g. corporate colour palate, upload company logo, etc)?	No. GenIA-L uses standard Indicator/Lefebvre branding and does not currently allow customers to upload their own logo or define customer-specific colour palettes or UI branding.	Noted
5.03	Does the system have a similar look and feel and overall consistency between screens and modules?	Yes. GenIA-L uses a consistent conversational interface across available content areas and document-analysis features, with common navigation, prompt entry, upload controls and response presentation.	Confirmed
5.04	Is data entry easily repeated if similar to previous entry?	Partially. Users can repeat similar requests by reusing or copying prompt wording and uploading similar document types. GenIA-L does not provide transaction-entry templates or stored default values in the way an accounting system would, because it does not maintain accounting records.	Noted - Additional question asked in 7.20
5.05	Does the software prevent access to a record while it is being updated?	N/A for accounting records. GenIA-L does not maintain shared customer records that users update concurrently. Each prompt/upload request is processed independently, so record locking is not required for user data entry. Platform administrative changes are restricted to authorised personnel.	Noted
5.06	Is there locking at file or record level?	N/A for user records/files because GenIA-L does not provide persistent customer file or record editing. Uploaded files are session/request scoped and not shared as editable records.	Noted
5.07	Does the software allow for the running of reports whilst records are being updated?	N/A for traditional reports and record updates. GenIA-L does not update accounting records while reports run. Users can submit on-demand prompts independently, subject to platform rate limits and service availability.	Noted
5.08	Can timestamps or user comments be added to transactions?	No user comments are added to accounting transactions because GenIA-L has no transaction records. Technical logs record request metadata such as user, time, device/session and status for security and operational purposes. Users may include context or comments in the prompt itself.	Noted
5.09	Is there the ability to store preferences and default values on a per-user basis e.g. department/team/user?	GenIA-L does not currently provide customer-defined default values, departments or team-specific data-entry defaults because the product is prompt based and does not maintain transactional forms.	Noted
5.10	Does the system have the ability to provide user-defined fields with associated validation of data input?	No. GenIA-L does not provide user-defined data-entry fields with associated validation. The system validates prompts and uploaded files, but users cannot define new structured fields in the application.	Noted
5.11	Can the system provide users with reminders and notifications e.g. workflows?	No. GenIA-L does not currently provide workflow reminders, task routing or approval notifications. Support or commercial communications are handled outside the application.	Noted
5.12	If the system provides workflows, does it have functionality to substitute/delegate authorisations?	N/A. GenIA-L does not provide workflow authorisation or approval routing, so substitute/delegated authorisations are not applicable.	Noted

Ref	Requirement	Response	Reviewer Comments
5.13	Describe the tools and features available for a power user to make configuration changes such as amending a workflow.	N/A. There is no customer-configurable workflow engine. Administrative configuration is limited to user access/subscription management and is controlled by authorised administrators.	Noted
5.14	Is there the ability for users to define and configure layouts of letters and forms?	No. GenIA-L can generate draft emails, reports or narrative content in response to prompts, but it does not provide a form/letter layout designer where users define and store templates inside the application.	Noted
5.15	Can users save the parameters of searches?	No. Search is carried out through ad hoc natural-language prompts. Users can manually reuse prompt wording, but GenIA-L does not currently save search parameters, filters or queries as reusable system objects.	Noted
5.16	Does the system have a "universal search" option, allowing a search to be undertaken over all modules of the system?	Yes, in the GenIA-L sense. The conversational search/retrieval capability searches across the curated Indicator/Lefebvre knowledge base and content areas available to the user under their subscription/entitlement. It is not an open-web search and it does not search customer systems. Uploaded documents can be included as context for the current request where the upload feature is used.	Confirmed
5.17	Can the system store menu option 'favourites' on a per user basis?	No. GenIA-L does not currently provide menu-option favourites. The product uses a single conversational interface rather than a large menu structure.	Noted
5.18	Can a user open multiple windows accessing the same or different modules of the system?	Yes, as a browser-based SaaS application, a user may open GenIA-L in more than one browser tab/window subject to session management and rate limits. Each prompt/upload request is processed independently.	Confirmed
5.19	Can more than one software function be performed concurrently?	The platform processes independent user requests concurrently across users. For a single user, concurrent prompts/uploads may be limited by session and rate controls; there are no accounting functions or batch processes running concurrently against shared records.	Noted
User documentation and training			
5.20	Confirm whether a user manual / instructions is provided and how this is distributed?	Yes. User instructions are provided electronically through the online help centre/knowledge base, onboarding documentation, product training materials and in-product guidance. The guidance covers the principal GenIA-L functionality, prompting, document analysis, source verification, security and privacy considerations, and common validation or processing issues. Customers may also receive onboarding sessions, webinars and customer-success support. Online and in-product guidance is updated centrally, so users do not need to install revised documentation. Material changes may also be communicated through product announcements, release notes, account-management communications, training updates or webinars.	Confirmed

Ref	Requirement	Response	Reviewer Comments
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 available user guidance includes: - Index or search facility: the online help centre/knowledge base provides searchable guidance. - Guide to basic functions: documentation explains the principal conversational research, prompting, source-review and document-analysis functions. - Pictures of screens and layouts: guidance includes screenshots and interface walkthroughs. - Examples: worked examples and sample prompts are provided for common research and document-analysis tasks. - Error messages: in-product validation and error messages explain common upload, file-format, file-size and processing problems, with additional guidance available through support materials. - Users can also obtain assistance through customer-success and support channels.	Confirmed
5.22	Is context-sensitive help available within the system?	General user documentation, onboarding materials and support channels are available separately.	Confirmed
5.23	Is the manual and/or help editable by the user (subject to the permissions matrix)?	No. User help and documentation are maintained by Indicator/Lefebvre and are not editable by customer users.	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)?	No detailed program documentation, source code, file definitions or escrow materials are made available to customers as standard. GenIA-L does not expose customer-facing APIs or file definitions for third-party links unless separately agreed. User documentation and support materials are provided instead.	Noted
5.25	Please detail the training options available?	Training is provided by Indicator/Lefebvre through sales, customer success/loyalty and support teams: product demonstration, onboarding session, user guidance, webinars or tailored training for customer teams.	Noted
5.26	Who provides training: - Software House? - VAR?	Software House / Indicator-Lefebvre provides training directly.	Noted
Support and maintenance			
5.27	How is the software sold: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	Direct from software house	Noted
5.28	How is the product supported: - Direct from the software house? - Via a Value Added Reseller (VAR) or Integrator?	Direct from the software house through customer services, account management and internal technical escalation.	Noted
5.29	Do VARs have to go through an accreditation process?	No, because the product is currently sold and supported directly.	Noted
5.30	Is the software sold based upon number of named users or a number of concurrent users?	Named users	Noted

Ref	Requirement	Response	Reviewer Comments
5.31	The supplier should detail the support cover options available, covering: - The hours provided? - Associated costs? - The global regions covered?	Standard support is provided Monday to Friday during UK business hours, excluding UK public holidays. Regions covered: UK customers supported by UK customer service, account management and product teams, with escalation available to wider Lefebvre technical resources where required Standard support is included within the GenIA-L SaaS subscription and no separate fee applies for normal support services. Any separately commissioned consultancy, bespoke training or non-standard professional services may be subject to separate agreement and charges. This support cover applies to UK customers and is provided by UK customer service, account-management and product teams. Issues may be escalated to wider Lefebvre product, engineering and security resources in other European locations where specialist assistance is required. The technical platform is continuously monitored outside customer-support hours, but this should not be interpreted as a 24x7 end-user support service unless separately agreed.	Noted
5.32	Detail the process by which customers raise support requests and how these can be viewed/managed?	Customers raise support requests by contacting customer services or their account manager by email/phone. The request is logged as a ticket, triaged by severity, assigned to the relevant support/product/engineering team, tracked to resolution and escalated where required. State whether customers can view ticket status directly or receive updates via support/account manager.	Noted
5.33	Please note the methods of support available: - Telephone? - Internet chat? - Remote access to customer workstation? - Other, please specify?	The following support methods are available: - Telephone: Yes, during the applicable support hours. - Email: Yes. - Internet chat: No dedicated live-chat support service is currently provided. - Remote access or screen sharing: Remote assistance may be provided where required and with the customer's express agreement, normally through a controlled Microsoft Teams screen-sharing session. - Other methods: Customer-success onboarding sessions, training webinars, account-management support and escalation to product or engineering specialists are available where appropriate.	Noted
5.34	Do you offer service credits for failure to meet performance around SLA and uptime (if applicable)	No service credits are currently offered for SLA/uptime failures unless separately agreed in the customer contract.	Noted
5.35	What is your escalation path for tickets which have not been resolved within a reasonable time?	Support ticket owner -> Customer Services Manager/Account Manager -> Product/Engineering lead for technical issues -> senior management/CIO for unresolved or critical incidents.	Noted

Ref	Requirement	Response	Reviewer Comments
5.36	How often are general software enhancements provided?	GenIA-L is continuously developed as a managed SaaS platform. General enhancements, bug fixes, security updates and functionality improvements are released throughout the year rather than according to a single fixed annual release schedule. All changes follow controlled development, testing, approval and deployment processes. Changes are tested in isolated development environments and then in an integrated pre-production environment before production deployment. Automated deployment gates prevent release where required validation has not been completed successfully. Updates are deployed automatically, so customers always use the current supported version and do not need to install upgrades. Material changes may be communicated through product announcements, release notes, account-management communications, updated documentation, training materials or webinars. For material product changes, customers may receive:	Noted
5.36 cont.		Product announcements Release notes Account-management communications Training updates Webinar briefings where appropriate	Noted
5.37	Will they be given free of charge?	Enhancements and bug fixes are generally included as part of the SaaS subscription unless they relate to separately priced modules or packages.	Noted
5.38	How are enhancements and bug fixes provided to customers?	Enhancements and bug fixes are deployed automatically to the SaaS platform. Customers do not need to install updates. Material changes or planned maintenance should be communicated according to the release/maintenance process.	Noted
5.39	Is "hot line" support to assist with immediate problem solving available?	No dedicated customer emergency hotline is offered beyond standard support channels, unless separately contracted. Critical service incidents are handled through internal operational escalation.	Noted
5.40	If so, is there an additional cost involved?	N/A because no separate hotline support service is offered.	Noted
5.41	At what times will this support be available?	N/A because no separate hotline support service is offered. Standard support hours should be stated in 5.31.	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 / Not applicable in the traditional modular sense. GenIA-L is accessed through a single browser-based conversational interface. Available content areas and document-analysis capabilities are integrated without customer setup beyond subscription/user access.	Noted
5.43	Are they integrated on real time basis or batch basis?	Real-time/on-demand. User prompts and document-analysis requests are processed interactively. There is no customer batch integration between separate modules.	Noted
5.44	Can the software be linked to other packages e.g. word processing, graphics, financial modelling, to provide alternative display and reporting facilities?	No direct live links to word processors, graphics tools or financial modelling packages are provided. Users may copy generated text into external tools and may upload supported documents/spreadsheets for analysis where permitted.	Noted

Ref	Requirement	Response	Reviewer Comments
5.45	Can definable links to spreadsheets be created?	No. GenIA-L does not create persistent or definable live links to spreadsheets and does not maintain synchronised connections to Excel workbooks or spreadsheet data. Where a supported file can be uploaded for analysis, it is processed as a standalone document for the active request. It is not linked to its original source, automatically refreshed, synchronised or used to update external spreadsheet cells or formulas.	Noted
5.46	Does the system provide a secure document storage capability: If so, please give examples of the document types saved and what transactions these might relate to.	No. GenIA-L does not provide a secure document-storage repository or document-management system. Users may upload supported documents for analysis during an active request or session. Uploaded documents are processed transiently and are not retained as persistent customer records or associated with accounting transactions. Customers remain responsible for storing their source documents and final outputs within their own document-management or business systems.	Noted
5.47	Can documents be scanned into a secure repository?	No. GenIA-L does not provide functionality for scanning documents directly into a secure repository, because it is not a document-management or document-storage system. Existing scanned documents or images may be uploaded where the relevant file type and content are supported, but only for transient analysis during the active request. They are not retained as stored repository documents after processing.	Noted
5.48	Does the system provide data migration tools for transactional and master data sets (e.g. employees customers, suppliers, journals, invoices).	No. GenIA-L does not provide data-migration tools for transactional or master datasets such as employees, customers, suppliers, journals, invoices, nominal ledgers or accounting records. GenIA-L is a professional research and document-analysis service and does not maintain the accounting, ERP, CRM or payroll datasets that would require migration tooling.	Noted

Ref	Requirement	Response	Reviewer Comments
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?	GenIA-L does not currently provide customer-facing web services, APIs, database connections or integration mechanisms that allow customers to add, update or delete transactional or master data. Customer access is provided through the authenticated browser application. The operations available to users include: - Submitting natural-language queries. - Retrieving and reviewing professional content. - Uploading supported documents for transient analysis. - Asking follow-up questions within an active conversation. - Generating and copying structured responses. GenIA-L can access the professional content available under the user's subscription and the prompt or supported documents submitted for the active request. It does not access or modify customer accounting transactions, journals, invoices, employee records, customer/supplier master data or external software databases. Internal integrations with identity, cloud-hosting, monitoring and AI-processing providers are managed by Lefebvre/Indicator and are not	Noted
5.50	Does the system support mobile working?	Yes, via estándar mobile browser. There is no native mobile app.	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.		
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?	GenIA-L is delivered as a cloud SaaS application hosted on Amazon Web Services (AWS) infrastructure located in the European Economic Area. AWS operates the underlying data-centre facilities and cloud infrastructure. Lefebvre/Indicator controls the GenIA-L application layer, user access, configuration, release management, monitoring, and the use of its approved subprocessors: AWS for hosting, Azure AD B2C for identity management and OpenAI for LLM processing.	Noted
6.02	Does the customer get a choice of the jurisdiction in which their data resides?	No. Customers are not offered an individual choice of data-residency jurisdiction. GenIA-L is operated from EU/EEA-hosted infrastructure and is designed to process customer prompts and uploaded documents transiently, without persistent storage or reuse for model training. This model supports GDPR compliance and avoids tenant-level customer data-residency configuration.	Noted - Additional question asked in 7.44
6.03	What certification(s) do you or your platform operators hold relating to your data centres and your business operations?	GenIA-L uses AWS as cloud platform operator. AWS maintains internationally recognised cloud and data-centre assurance certifications, including ISO 27001 and SOC 1/SOC 2 assurance reports. Lefebvre/Indicator applies application-layer security controls over GenIA-L, including strong authentication, RBAC and least privilege, API gateway token validation, centralised logging, monitoring, secure release management and GDPR privacy-by-design controls.	Noted
6.04	Do you or your platform operator have an SSAE16 (System and Organisation Controls) report available?	Yes. AWS SOC reports and related assurance materials are available through AWS standard assurance channels, including AWS Artifact, subject to the applicable access terms. Lefebvre/Indicator provides relevant platform and application-control evidence during customer or accreditation due diligence.	Noted
6.05	What are the physical controls over the:- - Premises? - Fileservers? - Communications equipment?	Physical controls over premises, server hardware and network communications equipment are operated by AWS. These include controlled data-centre access, security monitoring, environmental protection, resilient power and network infrastructure, and secure hardware and media handling. GenIA-L does not host customer systems in Lefebvre/Indicator-owned physical premises; Lefebvre/Indicator manages application, identity, access, monitoring and configuration controls above the AWS infrastructure layer.	Noted

Ref	Requirement	Response	Reviewer Comments
6.06	Is the space in this/these data centre(s) shared with any other companies?	Yes. AWS cloud data centres are shared facilities used by multiple AWS customers. GenIA-L does not rely on dedicated physical data-centre space. Customer access and processing are separated through AWS cloud isolation controls and GenIA-L application controls, including authenticated sessions, tenant and user entitlement checks, logical request isolation, encryption and restricted administrative access.	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?	GenIA-L is a multi-tenant SaaS service. It does not maintain a traditional customer accounting database containing ledgers, journals or master data. Persisted platform data is logically partitioned by customer account and user entitlement, while prompts and uploaded documents are processed as discrete transient requests. Security logs and operational metadata are centrally managed with access restricted to authorised technical administrators.	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?	Each user accesses GenIA-L through a unique authenticated account. Entitlements are linked to the customer's subscription and to individual user profiles. Server-side controls verify authentication tokens, session state and subscription entitlement before a user can access content, submit prompts, upload documents or view generated outputs. Administrative access uses named accounts, RBAC, least privilege and MFA.	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?	Cross-customer access is prevented by server-side authorisation checks, subscription entitlement validation, session isolation, API gateway token validation, RBAC for privileged access and centralised logging. Users do not receive direct database, file-system, ODBC, API or storage access. Customer prompts and uploaded documents are not persisted as shared files and are not available for retrieval by other customers.	Noted
6.10	How is [Internet] communication traffic monitored to identify potential problems before they happen: - From a performance perspective? - From a security standpoint?	Internet-facing traffic, service health and security events are monitored through infrastructure monitoring, application performance monitoring and security alerting. Monitoring covers availability, resource use, request behaviour, errors, authentication events and suspicious activity. Alerts are routed to designated technical teams for investigation and remediation, with activity and security logs centrally retained.	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?	GenIA-L does not post accounting transactions, maintain a ledger or commit transactional records. A prompt, document upload or AI-processing request is handled as a discrete operation. A network interruption, timeout or failed upload causes the request to fail safely or require re-submission; partial prompts or incomplete file transfers are not silently committed as valid records. Completed outputs are returned to the browser only after successful processing.	Noted

Ref	Requirement	Response	Reviewer Comments
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. Communications between the user's browser and the GenIA-L service are encrypted using HTTPS/TLS for login data and all application traffic, including prompts, uploaded documents, generated outputs and session communications.	Noted
6.13	Is data on your servers encrypted at rest?	Yes. Persisted platform data, logs, configuration, storage objects and backups used to operate the service are encrypted at rest using AWS-managed encryption controls. Customer prompts and uploaded documents are processed transiently and are not retained as persistent customer data.	Noted
6.14	What level of encryption is used?	Data in transit is protected with HTTPS/TLS. Data at rest in AWS-hosted storage, databases, logs and backups is protected using AWS encryption mechanisms and managed key controls. Passwords are managed by Azure AD B2C and are not stored in clear text by GenIA-L; password protection uses industry-standard hashing and encryption mechanisms.	Noted
6.15	Is a staging environment provided that is an exact replica of production; which can be used for testing purposes?	Yes. GenIA-L uses controlled non-production environments for testing and release validation before changes are deployed to production. These environments mirror the production architecture sufficiently to validate application behaviour, security controls and integration flows, while avoiding the use of live customer prompt or uploaded-document content.	Noted
6.16	Is a test environment provided to test configuration changes? If so, is there an additional charge for this?	Yes. Internal test and UAT environments are used to validate configuration, infrastructure and application changes before production release. These environments are operated by Lefebvre/Indicator for service assurance and are not charged to customers as a separate customer environment.	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?	GenIA-L operates under GDPR and Data Protection Act principles of privacy by design, data minimisation and restricted processing. The service is not intended to process personal data by design, but users can include personal data in prompts or uploaded documents. Mitigations include EU/EEA hosting, transient processing, no reuse of user data for model training, no persistent storage of prompts or generated responses, controlled subprocessors, access logging, RBAC and least-privilege administration.	Noted
6.18	Are you subject to any legal or regulatory requirements obliging you to retain a copy of customer data?	No. GenIA-L is not subject to a product-specific legal or regulatory requirement to retain customer prompts, uploaded documents or generated AI responses. Account, subscription, billing, support, security and operational log records are retained only for legitimate contractual, operational, security and legal purposes under Lefebvre/Indicator retention policies. Customer prompt and uploaded-document content is not retained as a customer data repository.	Noted

Ref	Requirement	Response	Reviewer Comments
6.19	Who will be able to access or see customer data?	Customer prompt content, uploaded documents and generated outputs are visible to the authenticated user during the active session or request. They are not made available to other customers and are not reused for model training. Authorised Lefebvre/Indicator technical staff can access operational metadata, security logs and system diagnostics for support, security and service operations. Privileged access is restricted, logged and controlled. Approved subprocessors process data only for the purpose of delivering the service.	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.	Internal access is controlled through named accounts, RBAC, least privilege, MFA for administrative access, secure identity management, API gateway controls, centralised logging and monitoring. Direct access to underlying storage and infrastructure is restricted to authorised technical administrators. Contractor and staff access is granted only for approved roles and is removed through joiner/mover/leaver controls. Security logs record privileged activity and security events.	Noted
6.21	Explain the release management procedures in place and the associated segregation of duties ?	Release management uses a controlled software delivery process with version control, peer review, test validation, controlled deployment and traceable change records. Development, review and deployment responsibilities are segregated through role-based permissions. Changes are promoted through non-production environments before production release, and production deployment is restricted to authorised personnel.	Noted
6.22	Is there sufficient segregation of duties preventing system developers from accessing and changing live applications and data files?	Yes. Developers do not have unrestricted live production access. Production access is limited to authorised personnel under RBAC and least privilege, with MFA for administrative access, logging of privileged activity and monitored change execution. Application code changes follow the controlled release process rather than direct manual modification of live application files or customer data.	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?	Emergency changes are handled through an incident or emergency-change process. The change is assessed, approved by authorised technical management, implemented by authorised operations staff, logged, tested and reviewed after implementation. The process preserves segregation of duties during the emergency and requires retrospective review where urgent action precedes full normal governance.	Noted
6.24	Is an audit trail always maintained of these emergency changes?	Yes. Emergency changes are recorded through change records, deployment logs, infrastructure logs and administrative activity logs. The audit trail captures the person or service account, timestamp, affected component, change description and outcome, and is retained centrally with restricted access.	Noted

Ref	Requirement	Response	Reviewer Comments
6.25	What procedures are in place when members of staff leave to ensure that their system access is stopped?	When staff or contractors leave or change role, their access is removed or amended through the joiner/mover/leaver process. Access to identity systems, code repositories, cloud consoles, monitoring tools, support systems and production environments is disabled or reduced according to role. Privileged accounts are named, controlled and logged, and access reviews support removal of obsolete permissions.	Noted
Platform and service levels			
6.26	Which databases and servers are used to host the software?	GenIA-L is hosted on AWS using cloud-native compute, containerised services and Infrastructure-as-Code. The service uses Kubernetes-based application components, AWS-hosted storage and database services for platform metadata, logs and configuration, and controlled integrations with Azure AD B2C for identity and OpenAI for LLM processing. Customers do not install or operate any servers.	Noted
6.27	What forms of user authentication are supported e.g. user names, passwords certificates, tokens etc.?	GenIA-L supports individual user IDs and password-based authentication managed through Azure AD B2C. Customer SSO integration is supported where the customer's Identity Provider uses OpenID Connect or SAML. MFA is enforced for technical administrative access. Sessions are controlled through authenticated tokens and expire after the defined session period or when the browser is closed.	Noted
6.28	What is the proposed product/service availability percentage?	The product availability objective is continuous 24x7 service availability. The service is designed for high availability through AWS cloud infrastructure, Kubernetes, Infrastructure-as-Code, monitoring and rapid reconstruction of the environment.	Noted
6.29	What percentage availability has been achieved over the past 12 months?	Availability is monitored through infrastructure and application monitoring. Customer-impacting incidents are handled through technical monitoring, alerting and support escalation, with standard internal recovery for common service issues targeted at under 1 hour and major database-related issues targeted at under 4 hours. ----- GenIA-L production availability is continuously monitored through Better Stack, which tracks uptime and health across the Kubernetes environment. Prometheus/Alertmanager and Grafana provide supporting monitoring of error rates, latency, throughput and infrastructure performance. For the 12-month period from 01/06/2025 to 30/06/2026, the measured production availability achieved was 99,9%. This figure is based on Better Stack uptime records.	Noted

Ref	Requirement	Response	Reviewer Comments
6.30	Is a service level agreement ("SLA") offered regarding: - Service availability? - Data recovery?	The service is operated with internal service-restoration targets: common internal service issues are typically recovered in under 1 hour, and major database-related incidents are targeted for recovery in under 4 hours. Recovery focuses on restoring service availability because GenIA-L does not maintain customer accounting transactions or persistent customer prompt/upload repositories.	Noted
6.31	Is the service available 24x7 or are there downtime periods for maintenance?	The application is available to customers 24x7 via a supported browser. Planned maintenance and production releases are performed as managed SaaS operations, with maintenance windows or customer communications used for material service-impacting changes.	Noted
6.32	Is the customer made aware of maintenance periods in advance?	Yes. Customers are notified in advance of material planned maintenance or changes expected to affect service availability. Routine non-disruptive releases and maintenance are applied automatically and do not require customer action.	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?	No client software is required. GenIA-L works entirely within supported internet browser software on the user's device. Users require a current version of Chrome, Edge, Firefox or Safari, a stable broadband connection and sufficient connection speed for document uploads.	Confirmed
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?	Not applicable as a downloaded executable is not used. GenIA-L is accessed through a browser and does not require customers to install a local executable program on their computers.	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 unsupported or end-of-life customer-side technology is required. Users access GenIA-L through current versions of mainstream supported browsers. Server-side components are maintained through the controlled release, patching and infrastructure management processes described in this section.	Noted
Platform security			
6.36	What security steps are taken to prevent and detect intrusion attempts?	GenIA-L uses layered controls to prevent and detect intrusion attempts, including HTTPS/TLS, API gateway token validation, request filtering, authentication, RBAC, MFA for administrative access, restricted direct infrastructure access, WAF and firewall controls, centralised logging, monitoring, security alerting and controlled release/patch management.	Noted
6.37	Is firewall hardware and software used to protect the live systems from unauthorised access?	Yes. The live AWS-hosted environment is protected by cloud network controls, firewall and security-group rules, and application gateway controls that restrict inbound and administrative access. Direct access to underlying infrastructure and storage is restricted, and all user access is mediated through the authenticated browser application and API gateway.	Noted

Ref	Requirement	Response	Reviewer Comments
6.38	Which monitoring software is used to create alerts when intrusion attempts are suspected?	Alerts are generated from AWS-native monitoring services together with Lefebvre/Indicator's internal IT monitoring and security alerting tools. The monitoring covers authentication events, administrator activity, application errors, service availability, resource usage, anomalous request behaviour and security violations, with alerts routed to the technical teams responsible for response.	Noted
6.39	Are designated staff responsible for receiving and urgently responding to these alerts?	Yes. Designated technical and security staff receive and respond to monitoring and security alerts. Alerts are triaged according to severity, investigated by the relevant operations or security team, escalated through support or technical management when required, and recorded through internal ticketing or incident records.	Noted
6.40	Have clear procedures been established for identifying and responding to security incidents?	Yes. Security incident procedures are established for detection, triage, containment, remediation, recovery, logging and communication. Security events from access controls, infrastructure and application monitoring are analysed and escalated according to severity. Customer communication is handled through support/account channels and legal/privacy escalation where an incident affects customer data or service availability.	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. Security-sensitive software, including operating-system images, runtime components, container images, databases, managed cloud services and application dependencies, is kept up to date through the controlled patching and release process. Critical security patches are prioritised and applied through emergency or accelerated change procedures; routine patches are applied through standard release cycles.	Noted
6.42	List the procedures and software tools in place to prevent or detect and eliminate interference from malicious code, such as viruses?	Malicious-code risks are addressed through file upload restrictions, file-type and size validation, malware checks in the upload and processing pipeline, input validation, request filtering, dependency management, container image controls, security monitoring and controlled deployment pipelines. Uploaded documents are processed for the user request and are not stored as persistent shared files. Suspicious or malformed inputs are rejected or fail safely and relevant errors are logged.	Noted
6.43	Is a system log maintained by the service provider that details - User access? - User activity? - Error messages? - Security violations?	Yes. The service provider maintains centralised logs covering user login and security events, administrator activity, read/write operations across infrastructure layers, application errors, system health events and security violations. Logs cannot be disabled by ordinary users and are protected for confidentiality, integrity and availability.	Noted

Ref	Requirement	Response	Reviewer Comments
6.44	Is this log available to the customer?	Not as a self-service customer-facing log within the application. Customer administrators can request user/subscription access information and support can provide relevant incident or access information through the support process where appropriate. Internal security and infrastructure logs remain restricted to authorised Lefebvre/Indicator personnel to preserve platform security and confidentiality.	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 successful unauthorised access attempt has been recorded in the information used for this accreditation response during the last year. Unsuccessful or suspicious attempts are handled through monitoring, security alerting, logging, investigation and remediation processes.	Noted
6.46	Is penetration testing regularly carried out by (please indicate frequency of tests): - Staff specialising in this field? - External specialists?	Yes. Security testing is carried out on a periodic and change-driven basis by staff with security responsibilities and specialist resources. Testing includes review of internet-facing components, application controls, infrastructure configuration and release changes. Findings are tracked through the remediation process until closure.	Noted
6.47	Are procedures in place to ensure that any weaknesses found by penetration testing are addressed quickly?	Yes. Weaknesses identified by penetration testing, security review, monitoring or vulnerability assessment are recorded, prioritised by risk, assigned to an owner, remediated through the controlled change process and verified before closure. Critical issues follow accelerated remediation and escalation.	Noted
6.48	If penetration testing by a specialist is not performed regularly, please indicate the main procedures in place to identify weaknesses?	Specialist penetration and security testing is supported by additional continuous controls: secure SDLC, code review, dependency and image review, infrastructure configuration review, monitoring, centralised logging, access reviews, patch management and incident-response procedures. These controls provide ongoing detection and remediation of weaknesses between formal tests.	Noted
6.49	Are security procedures regularly reviewed? Please indicate frequency of reviews.	Yes. Security procedures are reviewed regularly through operational security management, release/change governance, incident reviews, access reviews and compliance activities. Security-relevant policies and controls are updated when risks, architecture, regulations or operational lessons change.	Noted
6.50	What security reporting is provided demonstrating compliance against certification(s) and policy(ies)?	Security reporting includes AWS assurance evidence for the hosting environment, centralised access and activity logs, security-alert records, incident records, change/deployment records, access review evidence, vulnerability/remediation records and GDPR/subprocessor documentation. Certification evidence relating to AWS is available through AWS assurance channels.	Noted

Ref	Requirement	Response	Reviewer Comments
6.51	How are security breaches communicated to customers?	Security breaches affecting customers are communicated through customer support/account-management channels and formal notification processes. Communications include the nature of the incident, affected services or data, known impact, mitigation actions, customer actions required and updates through closure. Personal-data incidents are escalated through the privacy/DPO process and handled in line with GDPR notification obligations.	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?	GenIA-L does not back up customer prompts, uploaded documents or generated responses as customer records because these are processed transiently and are not retained as a persistent repository. The service backs up the platform components required to operate and restore the SaaS service, including application configuration, infrastructure definitions, platform databases/metadata, logs and subscription/account data. Backups use scheduled and versioned AWS-managed encrypted storage and snapshot mechanisms, are stored within the controlled AWS environment, are access-restricted to authorised operations/security staff and are retained under operational and security retention schedules.	Noted
6.53	How frequently is a test-restore of backups undertaken?	Test-restore and recovery exercises are undertaken as part of service recovery validation, release assurance and operational readiness activities. The recovery approach is based on restoring platform services from Infrastructure-as-Code, Kubernetes deployment definitions, AWS-managed data backups and operational configuration, rather than restoring customer prompt/upload content. ----- Test-restore and recovery exercises for the backups used to recover GenIA-L platform services and operational data are performed at least annually, and additionally following material changes to the backup or recovery process. The exercises verify that the relevant backups can be restored and that the recovered services and operational data are usable. Results, exceptions and corrective actions are documented and reviewed.	Noted
6.54	Can the provider restore from a backups that it has taken at a customer request?	No. GenIA-L is not a customer data repository and does not restore historical customer prompts, uploads or generated responses at customer request. Provider restores are used to recover the SaaS platform and operational data after service incidents. Customers retain and manage their own source documents and saved outputs outside GenIA-L.	Noted

Ref	Requirement	Response	Reviewer Comments
6.55	Does a customer have the ability to undertake their own backups?	Customers do not perform system-level backups of GenIA-L because they do not manage the SaaS infrastructure or database. Customers can save, download or copy outputs and retain their original uploaded documents within their own systems according to their internal backup policies.	Noted
6.56	If so, can a customer restore data a backup that they have taken?	Customers cannot restore data into the GenIA-L SaaS platform from their own backups. They can re-upload source documents, re-submit prompts and use saved outputs or documents from their own systems. GenIA-L does not import customer backup files to recreate a historic application state.	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?	Service recovery is based on AWS cloud resilience, Kubernetes, Infrastructure-as-Code, controlled deployments, monitoring, alerting and restoration of platform components from backups and configuration. Database or application corruption is addressed through rollback, redeployment and restoration of operational data. Hardware failure, theft, fire, flood and data-centre events are mitigated by AWS infrastructure controls. Communication failures are handled through monitoring, retry/error handling and service restoration procedures.	Noted
6.58	How often are these plans tested?	The Business Continuity and Disaster Recovery arrangements applicable to GenIA-L are formally tested at least annually and additionally following significant architectural or operational changes or a major incident. The test and its results are documented, and identified corrective and preventive actions are assigned to responsible owners and tracked through the continuous improvement process. In addition to the formal exercise, recovery controls are subject to ongoing operational validation under the AI System Lifecycle Management Policy and AI System Lifecycle Management Procedure. All changes progress through isolated development and integrated pre-production environments before production, and deployment is blocked if any required validation fails. Production deployments are reversible to a tagged previous known-good state, with a documented RTO of less than four hours and a near-zero RPO.	Noted
6.58 cont.		GenIA-L is continuously monitored through Better Stack, Prometheus/Alertmanager and Grafana. Operational anomalies trigger a documented three-tier escalation process, and all incidents are logged, investigated and subject to post-incident review. Resulting corrective and preventive actions are reviewed by the Operational AI Committee and incorporated into the continuous improvement process.	Noted

Ref	Requirement	Response	Reviewer Comments
6.59	How often are these plans reviewed and updated?	Test restores of the backups used to recover GenIA-L platform services and operational data are performed at least once annually, and additionally following material changes to the backup or recovery process. The test verifies that the relevant backups can be restored and that the recovered services and operational data are usable. Results, exceptions and corrective actions are documented and reviewed. This backup-restoration process is complemented by the documented deployment rollback capability in the AI System Lifecycle Management Policy and AI System Lifecycle Management Procedure. Any production deployment can be returned to a tagged previous known-good version, with all relevant versions retained in Git and S3. The documented rollback objectives are an RTO of less than four hours and a near-zero RPO. Rollback authority rests with the Tech Lead, with notification to the AIMS Representative.	Noted
6.60	What is the longest period of time envisaged that service may not be available?	The longest envisaged customer-impacting outage is a major service incident requiring restoration of core platform components. Internal recovery targets recorded for GenIA-L are under 1 hour for standard internal service issues and under 4 hours for major database-related issues, excluding dependency outages caused by third-party services outside direct Lefebvre/Indicator control.	Noted
6.61	What are your: - Recovery Point Object (RPO) standards? - Recovery Time Objective (RTO) minimum standards?	RPO for customer prompts, uploaded documents and generated responses is not applicable as those items are not retained as persistent customer records. RPO for platform metadata and operational data is aligned to the most recent available encrypted backup or managed storage recovery point. RTO targets are under 1 hour for common internal service issues and under 4 hours for major database-related service incidents.	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?	System event timestamps are generated centrally by the service and stored consistently for audit, monitoring and troubleshooting. Server-side logs use central service time to ensure reliable correlation across infrastructure, security and application events. User-facing dates and times are presented in the application context rather than used as accounting transaction timestamps.	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?	GenIA-L is not the system of record for customers' accounting or business data. Customers retain their original accounting records, source documents and saved outputs within their own systems. Because prompts and uploads are processed transiently, customers are not dependent on GenIA-L to retrieve accounting records after a provider difficulty. Account/subscription records and operational data are managed under Lefebvre/Indicator contractual and retention procedures.	Noted

Ref	Requirement	Response	Reviewer Comments
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?	Full standby operation by another organisation is not provided to customers. The minimal customer-protection arrangement is that GenIA-L does not hold customers' source accounting records as a repository; customers retain source data and locally saved outputs independently of the service. AWS cloud resilience and Lefebvre/Indicator recovery procedures are used to continue or restore the SaaS service.	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?	GenIA-L hosting is provided through Lefebvre/Indicator's AWS environment. Customers do not contract directly with AWS for this service and do not take over the hosted environment. Continuity of hosting is managed through Lefebvre/Indicator's AWS relationship and cloud resilience model, with customer access governed by the GenIA-L subscription.	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. GenIA-L is operated by Lefebvre/Indicator using team-based ownership, documented cloud architecture, Infrastructure-as-Code, Kubernetes deployments, monitoring, logging and support/escalation procedures. No single employee's absence or departure would stop the provider's ability to operate and support the service.	Noted
Platform change management			
6.67	Describe your approach to upgrades including what option customers have not to take upgrades (if any)?	GenIA-L is upgraded as a centrally managed SaaS service. Customers do not install upgrades and generally cannot remain on older versions. Enhancements and bug fixes are deployed automatically by Lefebvre/Indicator through the controlled release process and are included as part of the service.	Noted
6.68	Are users able to test the application before new versions go into live use?	Customers are not required to test each release before live deployment. New versions are tested internally in controlled non-production environments before release. Routine fixes and enhancements are validated by Lefebvre/Indicator before customer availability.	Noted
6.69	Are users given notice before application changes are applied to the live system?	Yes. Customers are given notice of material application changes or planned maintenance that affect usage, availability or user behaviour. Routine non-disruptive fixes and enhancements are deployed automatically through the SaaS release process.	Noted
6.70	Are changes delivered into the live environment "switched off" to enable users to test them before enabling them for their environment?	Material capabilities can be introduced using controlled rollout practices so that Lefebvre/Indicator can validate behaviour before broad enablement. Routine fixes and security updates are deployed directly once they pass testing because customers do not manage separate production versions.	Noted

Ref	Requirement	Response	Reviewer Comments
6.71	Describe what testing and QA processes are undertaken before upgrades and other changes are made live/available to customers?	Before release, changes undergo peer review, automated and manual testing, validation in non-production environments, regression checks, security review for relevant changes, monitoring readiness and controlled deployment. AI-related changes are assessed against product behaviour, source traceability, input handling, output quality and safety expectations.	Noted
6.72	Explain the release management procedures in place and the associated segregation of duties?	Release management follows version-controlled development, peer review, build/deployment pipelines, non-production validation, authorised production deployment and traceable change records. Segregation of duties is enforced through role-based permissions so that development, approval and production operation are not performed as uncontrolled direct changes to live systems.	Noted
6.73	Are users informed when they next login of the application changes that have gone into live use?	Users are informed of material product changes through product communications, release notes, support/account communications or in-application messaging as appropriate. Routine fixes and security updates do not require user acknowledgement at next login.	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.	No customer regression testing or installation activity is required for standard releases, patches or upgrades. Customers access the latest version through the browser. Customers read release notes or adapt internal guidance where a material user-facing feature or workflow changes.	Noted
Subscription options			
6.75	What is the minimum level of commitment must the customer sign up to, e.g. 36 months?	GenIA-L is sold directly by the software house as a named-user SaaS subscription. The minimum commitment is the subscription term agreed in the customer order form; customers do not need to purchase infrastructure, install software or commit to a separate hosting contract.	Noted
6.76	Where online payment is used, what type of security is used to protect sensitive information?	Online card-payment processing is not performed inside the GenIA-L application. Subscription payment and invoicing are handled through Lefebvre/Indicator commercial and finance processes outside the product. Sensitive payment handling is therefore separated from the GenIA-L SaaS application.	Noted
6.77	Where online subscription / payment is used, is an invoice provided to the customer and, if so, in what format?	Yes. Customers receive an invoice for the subscription through Lefebvre/Indicator finance processes. Invoices are provided electronically in the standard format used for customer billing, typically PDF or electronic invoice format.	Noted
6.78	When subscriptions need to be renewed, what advance notice is provided and what is the time limit for renewal?	Renewal is managed through the Lefebvre/Indicator customer service, account management and finance processes before the subscription end date. Customers are contacted in advance of expiry and access remains subject to an active subscription or approved renewal.	Noted

Ref	Requirement	Response	Reviewer Comments
6.79	Is there a procedure for late renewal and is there a time limit after which subscriptions cannot be renewed?	Yes. Late renewal is handled through the customer service/account management process. Access can be suspended when the subscription is not renewed or payment is not received, and service access is reactivated following renewal approval and account re-enablement.	Noted
6.80	How soon after creating or renewing a subscription (if applicable) can the system / service be used?	After the subscription or renewal is confirmed, access is provisioned through the subscription administration and identity-management process. The service can be used once the named user account has been created or renewed and the user has authenticated in the browser.	Noted
6.81	What notifications / confirmations are provided to the customer regarding subscriptions and payments?	Customers receive commercial and service notifications, including order or renewal confirmation, user activation communications, invoice/payment communications, support updates and service communications for material maintenance or product changes.	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?	GenIA-L does not store customers' accounting records or source business data. Missed payments or termination can suspend access to the application and to the customer's active subscription entitlements. Customers continue to hold their original documents, accounting records and any outputs they saved or exported outside GenIA-L.	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?	At contract end there is no GenIA-L customer accounting database to extract because prompts and uploaded documents are not retained as a persistent repository. Customers are expected to save or export any outputs they require before access ends, while account and billing records are handled under Lefebvre/Indicator contractual and retention policies.	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?	Customer prompts and uploaded documents are discarded after processing in line with the zero-data-retention model and are not maintained as files requiring end-of-contract destruction. Generated responses are not retained as a customer document repository. Account, billing, support, security and legal records are retained or deleted under Lefebvre/Indicator retention policies. Destruction certification is not issued for transient prompt/upload content because it is not retained as end-of-contract customer data.	Noted
6.85	What is your processes regarding disposal of end-of-life and failed hardware devices that were used to operate your service?	End-of-life and failed data-centre hardware used for the AWS-hosted service is disposed of under AWS secure media and hardware disposal controls. Lefebvre/Indicator does not provide dedicated customer hardware for GenIA-L. Any internal corporate devices used by staff are handled through Lefebvre/Indicator secure asset disposal processes.	Noted

Ref	Requirement	Response	Reviewer Comments
SaaS/Hosted reporting			
6.86	Are reports produced from the same software as the financial applications or is separate reporting software used?	GenIA-L is not a financial application or accounting report writer. Outputs, summaries, comparisons and practical documents are produced within the same GenIA-L browser-based SaaS application, using the product's retrieval and AI-processing workflow. No separate customer-side reporting software is required.	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?	No. Users only require a supported web browser to prepare, view and interact with GenIA-L outputs. A PDF reader or office application is useful only for viewing files that the user downloads or saves outside the application.	Confirmed
6.88	What browser versions are support: - On desktop/laptop (PC, Mac, Linux)? - On Tablets? - On mobiles?	GenIA-L supports current versions of Chrome, Edge, Firefox and Safari on desktop and laptop devices. The application can also be used on tablets and mobiles through current mainstream mobile browsers, subject to screen size and stable internet connectivity. No specific operating system is required beyond support for a modern browser.	Noted
6.89	Is access to the reporting facilities and data controlled by the same procedures as access to the main application?	Yes. Access to generated outputs and reporting-style information within GenIA-L is controlled by the same authentication, session, subscription entitlement, RBAC and logging controls as the main application.	Noted
6.90	If it's different, explain the user access control facilities available to ensure information is only viewed by users with appropriate authority?	The access controls are not different. Generated outputs are part of the main GenIA-L application experience and use the same authenticated user session, subscription entitlement checks, security logging and browser access controls.	Noted
6.91	In what electronic formats are reports produced:- - PDF? - XML? - MS Excel spreadsheet? - CSV file? - As html for viewing in a web browser? - Other, please specify?	GenIA-L outputs are primarily produced as browser-viewable HTML/text with structured tables where relevant. Users can copy generated text and tables to office applications and use download/export functions provided by the interface for generated outputs. The product is not an XML-based accounting-reporting tool and does not generate statutory accounting report files.	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?	Generated outputs are viewed in the browser during the active session and are not stored by GenIA-L as a persistent web-server report-document repository. Users who need to retain an output store it in their own systems by copying or downloading it. Server-side operational logs contain security and diagnostic metadata rather than customer report documents.	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?	Normal browser cache or temporary files are controlled by the user's browser and device while viewing web content. Protection of the local device and browser profile is the customer's responsibility. GenIA-L protects the server-side session with authentication, session expiry and encrypted communications, and users must re-authenticate after logout or session termination.	Noted

Ref	Requirement	Response	Reviewer Comments
6.94	Are communications between the browser and the server encrypted for any report related communications?	Yes. All browser-to-server communications for prompts, document uploads, generated outputs and reporting-style interactions are encrypted using HTTPS/TLS.	Noted
6.95	If reports are produced dynamically each time the user views them can historical reports be reproduced at any time?	No. GenIA-L is not a historical report archive and does not retain prompts, uploaded documents or generated responses as permanent report documents. Users must save or export outputs they need to preserve. A user can submit a new prompt or re-upload source material to generate a fresh response, but that is a new output based on the current product and content context rather than a guaranteed reproduction of a prior report.	Noted
6.96	Can reports viewable in a browser be navigated dynamically by users? For example: - Enabling drill down to more detailed information? - Altering which columns and rows of data are displayed. - Choosing time periods? - Specifying selection criteria?	Yes, through the conversational interface. Users can ask follow-up questions, refine prompts, request comparisons, request tables or summaries and provide additional document context. GenIA-L does not operate as a traditional BI drill-down report writer with configurable accounting periods, columns or ledger hierarchies.	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. Text and structured tables displayed in the browser can be copied into Microsoft Excel or other office applications. Complex formatting remains subject to normal browser and spreadsheet behaviour, while tabular content is designed to remain understandable when copied or saved by the user.	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?	Yes. Failed uploads, timeouts, processing errors and interrupted requests are surfaced to the user through loading, error or retry behaviour rather than silently committing partial accounting records. The user can re-submit the prompt or upload. Because GenIA-L is not a ledger system, an incomplete request does not corrupt accounting transactions.	Noted

Ref	Requirement	Response	Reviewer Comments
7.	LEGAL INFORMATION & RESEARCH		
Gen AI Platform architecture			
7.01	Does the platform rely on a single large language model (LLM) interaction, or does it use a multi-step processing pipeline? (e.g. retrieval, ranking, generation, post-processing, etc)	GenIA-L uses a multi-step processing pipeline rather than a single unconstrained LLM interaction. The pipeline includes authentication and entitlement checks, input and file validation, query interpretation, retrieval and ranking of relevant passages from the approved Indicator/Lefebvre content corpus, response generation, source presentation and post-processing controls. User-uploaded documents may also provide request-specific context. The service does not perform open-web searches or use uncontrolled internet sources.	Noted
7.02	Where a multi-step pipeline is used, which components are deterministic versus probabilistic? For the user facing response, which elements are templated or fixed and which are dynamically generated?	GenIA-L uses a combination of deterministic controls and probabilistic AI components. Deterministic components include: - User authentication and subscription-entitlement checks. - Validation of supported file types and the applicable 10 MB and 150-page limits. - The decision to apply OCR when a document does not contain machine-readable text. - Request routing and restriction of retrieval to the approved Indicator/Lefebvre content corpus. - Application of predefined system instructions, security controls and product rules. - Presentation of interface labels, legal notices, file-validation warnings and source links.	Noted
7.02 cont.		Probabilistic or model-based components include: - Semantic interpretation of the user's question. - Identification and ranking of the content passages most relevant to the request. - OCR recognition where image-based documents require text extraction. - Natural-language generation, summarisation and analysis. - Automated LLM-as-judge assessments used to monitor response quality. For the user-facing response, interface wording, legal notices, validation messages, source-display structure and system guardrails are fixed or controlled. The substantive answer is dynamically generated from the user's prompt, active conversation context, uploaded-document content and retrieved professional sources.	Noted
7.02 cont.		GenIA-L does not select a complete pre-written answer from a fixed template. Because interpretation, retrieval ranking and response generation include probabilistic components, some variation in wording or emphasis may occur when the same question is submitted more than once.	Noted

Ref	Requirement	Response	Reviewer Comments
7.03	Which foundation model(s) is the platform based on?	GenIA-L currently uses OpenAI LLM services under a corporate agreement. Current product documentation identifies GPT latest models as the principal model used for response generation. The platform combines the foundation model with Lefebvre/Indicator's proprietary retrieval architecture, controlled prompts, evaluation framework and curated professional content. Model changes are controlled through the AI system lifecycle, evaluation, change-management and deployment processes before release to production.	Noted
7.04	Can customers select a foundation model if they do not wish to use a particular model supplier?	No. Customers cannot select an alternative foundation model or exclude a particular model supplier as a customer-level configuration option. Model and supplier selection is managed centrally by Lefebvre/Indicator under its approved technology, security, risk-assessment and change-management processes.	Noted
7.05	Does the platform use retrieval-augmented (RAG) techniques or other mechanisms to ground responses in authoritative sources? Please describe the architecture used and when each approach is applied.	Yes. GenIA-L uses retrieval-augmented generation to ground professional answers in approved Indicator/Lefebvre sources. The user's question is analysed, relevant content passages are retrieved and ranked, and the selected passages are supplied as grounding context for response generation. Source references are presented where available. For legal, tax and accountancy research, the principal grounding source is the curated professional content corpus. Where a document is uploaded, extracted document content may also be used as request-specific context, either independently or together with retrieved professional sources.	Noted
Data handling, retention and deletion			
7.06	How is customer data handled once submitted to the platform (including chat history, queries, results, saved searches/filters, and 'engagements'), particularly where content may be sensitive or confidential?	Customer prompts, uploaded documents and generated outputs are processed for the active request or session and are not maintained as a persistent customer repository in the current product. They are not used to train or fine-tune Lefebvre/Indicator or third-party foundation models. This zero-retention position applies to substantive customer content. GenIA-L separately retains the limited identity, subscription, technical, security and operational metadata required to authenticate users, operate and protect the service, investigate incidents and meet compliance obligations. Explicit feedback voluntarily submitted through the in-product feedback channel may also be retained for investigation and product-quality management.	Noted
7.07	What are the default retention periods for chat history, engagements, saved searches/filters, and results? Are these retention settings configurable by the customer/administrator?	The current default is zero persistent retention for prompts, uploaded documents, chat content and generated outputs. These items are available only for the active session and are automatically deleted when the session ends. GenIA-L does not currently provide persistent engagements, saved searches, stored filters or historical results.	Noted

Ref	Requirement	Response	Reviewer Comments
7.08	What capabilities are available to export user activity (e.g. queries, results, saved searches/engagements), and in what formats can this be provided?	GenIA-L does not provide a retrospective export of complete query, engagement or result history because this content is not retained after the active session. During the active session, users can copy response text and structured tables and save them within their own systems. The exact customer-facing download formats currently supported is docx.	Noted
7.09	If deletion is enabled by customer admin roles, does this deletion extend to backups?	Customer-admin deletion of chat history, engagements or saved results is not applicable to the current product because these items are not retained as persistent customer records. Accordingly, customer prompts, uploaded documents and generated outputs are not included in platform backups. Backups cover the operational components required to recover the SaaS service, including configuration, platform metadata, logs and subscription/account information. Those backups are subject to their own access, retention and deletion controls.	Noted
7.10	How is customer data segregated in your multi-tenant environment (logical segregation controls and any additional safeguards for sensitive data).	GenIA-L is a multi-tenant SaaS service. Tenant access is logically segregated through named authenticated accounts, subscription and content entitlements, session isolation, API token validation and role-based access controls for privileged operations. Users cannot access another customer's sessions, databases, storage, logs or file systems and do not receive direct database, ODBC or infrastructure access. Prompt and uploaded-document content is processed as transient request data rather than stored in a shared customer repository.	Noted
7.11	Does any customer content flow into observability, monitoring, or logging tools? If so, how is sensitive data prevented from being captured in logs or traces?	Customer prompt and document content is not intended to be captured in application, observability or infrastructure logs. Monitoring systems receive technical and security information such as authentication events, error codes, latency, resource utilisation, service health and alert status. Application logging is configured to exclude substantive prompt, document and response content. Access to logs is restricted through named accounts, least privilege and administrative controls.	Noted

Ref	Requirement	Response	Reviewer Comments
7.12	What are your audit log retention periods for both infrastructure logs and application logs?	GenIA-L does not currently apply a predefined time-based retention limit to infrastructure or application audit logs. The logs are retained for operational monitoring, service security, incident investigation and audit traceability and are not automatically deleted solely on the basis of their age. Their retention is subject to periodic review to ensure that it remains necessary and proportionate for its operational and security purposes. Logging is configured to capture technical, operational and security information. User prompts, uploaded-document content and generated responses are excluded from the application and infrastructure logs. Access to logs and monitoring records is restricted to authorised technical and security personnel through named accounts, role-based access controls and the principle of least privilege.	Noted
Sources, Jurisdiction coverage and updates			
7.13	What jurisdictions (UK etc.) and content types are covered (legislation, case law, regulations, guidance, manuals), and what are the key exclusions/limitations?	The UK version of GenIA-L is principally designed for UK tax and accountancy research, including income tax, corporation tax, VAT, capital gains tax and financial reporting. Depending on subscription entitlements, related coverage may include UK company law, payroll, employment/HR, and health and safety. Available content may include legislation and regulatory material, expert-authored commentary, technical guidance, manuals, newsletters, cases, templates, checklists and other Indicator/Lefebvre professional materials. Exact content availability depends on the customer's subscription. GenIA-L does not search the open web and is not intended for unsupported jurisdictions, general knowledge, non-professional advice or matters outside its available content corpus.	Noted
7.14	Is the model limited to only using approved sources? How is this enforced?	GenIA-L is configured to ground substantive professional answers in approved Indicator/Lefebvre content retrieved through its RAG architecture. It does not browse the open web or incorporate uncontrolled internet search results. Enforcement is applied through the controlled retrieval corpus, subscription entitlements, system instructions and response-generation workflow. User-uploaded documents may also be used as request-specific sources. As the foundation model remains probabilistic, professional verification of the answer and cited sources is still required.	Noted

Ref	Requirement	Response	Reviewer Comments
7.15	How are sources prioritised and presented within the platform, and what factors influence their ranking?	Sources are selected and ranked according to their relevance to the user's question, the available jurisdiction and content domain, the customer's subscription entitlements and the relevance of individual passages. Where available, metadata such as source type, date and applicability may also influence retrieval and presentation. Retrieved sources are presented as references or links alongside the answer so that the user can review the underlying material.	Confirmed
7.16	How does the system detect when there are insufficient or low-quality retrieval results? How does the model react and signpost this to the user?	When the retrieval process does not identify sufficiently relevant material, GenIA-L is configured to avoid presenting an unsupported conclusion and to indicate that the answer cannot be fully grounded in the available content. Users are encouraged to refine the question, provide additional context or verify the matter independently.	Noted
7.17	Are there potentially relevant sources of information that are not included in the model's review? How is this signposted to the user?	Yes. Potentially relevant information may be excluded where it falls outside the Indicator/Lefebvre corpus, the customer's subscription, the supported jurisdiction or domain, or the content available in the retrieval index at that time. This limitation is communicated through the defined product scope, source references and responsible-use guidance. The sources displayed with an answer show the material on which it has been grounded, but should not be interpreted as a guarantee that every potentially relevant external source has been considered.	Noted
7.18	Is there a time-lag between legal change and its availability in the solutions? And if so, what is the typical time-to-update after changes to UK legislation/regulations/guidance, and how is this communicated to the user?	A time lag may occur between a legal or regulatory change and its availability in GenIA-L because the change may require editorial review, content publication and technical ingestion or indexing. The current typical update target is no more than one week, although the timing depends on the nature and complexity of the change and is not presented as a contractual SLA. The publication or effective date of source material enables users to assess recency.	Noted
7.19	Can the platform handle effective dates, superseded versions, and historical snapshots (e.g., "law as at" a specific date)?	GenIA-L can respond to date-specific questions where the underlying content contains the relevant effective dates, superseded material or historical commentary and the user clearly identifies the required date. However, the platform does not currently guarantee a complete point-in-time historical snapshot of all applicable law. Users should state the relevant date explicitly and verify the resulting answer and sources, particularly where historical versions or transitional provisions are material.	Noted

Ref	Requirement	Response	Reviewer Comments
7.20	If the same query is run multiple times, how consistent is the response? (Including sources used, citations listed and estimated certainty rating.) How is this measured?	Repeated queries should be broadly consistent when the same prompt, conversation context, content corpus and production configuration are used. Some variation in wording, ordering and emphasis is expected because semantic ranking and natural-language generation are probabilistic. Source selection is constrained by the approved corpus, but retrieved passages and their order may also vary. GenIA-L does not currently display an estimated certainty rating. Repeatability is not currently reported as a customer-facing percentage or stability metric. Automated LLM-as-judge assessments monitor answer quality between releases.	Noted
7.21	How does the model treat contradictory sources?	When retrieved sources contain different or contradictory positions, GenIA-L is intended to present the relevant distinction rather than silently selecting one position. The response may distinguish sources according to date, jurisdiction, legal hierarchy, factual context or applicability and provide the relevant references for review. GenIA-L is not a deterministic legal conflict-resolution engine. Where the conflict cannot be resolved reliably from the available content, the uncertainty should be made clear and the user should apply professional judgement.	Noted
7.22	How does the system respond when the legal position is known to be unsettled?	Where the legal position is unsettled, GenIA-L is intended to identify the uncertainty, avoid presenting the matter as conclusively settled and refer the user to the relevant available sources or competing interpretations. The response should be treated as research assistance rather than a definitive legal opinion, and users are expected to verify the current position and exercise professional judgement before relying on it.	Noted
7.23	Are citations generated for sources? If so: - Are they generated using direct linking to retrieved passages or via post-generation matching of text to sources?	Yes. GenIA-L provides citations or source references based on material retrieved from the approved Indicator/Lefebvre corpus. These references are associated with the retrieved sources used as grounding context and are not produced through a generic open-web citation search. Users can follow the reference to review the underlying material, subject to their subscription entitlement.	Confirmed
7.24	Can the model return citations that are syntactically valid but semantically unrelated?	Yes. As with any probabilistic AI system, a residual risk remains that a citation may be syntactically valid but not fully support the associated statement. GenIA-L reduces this risk through retrieval from a controlled professional corpus, grounding in retrieved passages, source-reference presentation, automated quality evaluation and user access to the underlying material. Users are nevertheless expected to verify that each cited source supports the relevant conclusion.	Noted

Ref	Requirement	Response	Reviewer Comments
7.25	How are citations validated before being shown to users?	Citations originate from sources identified by the retrieval process and retain the relevant source identifier or link so users can inspect the underlying material. The controlled corpus reduces the risk of fabricated authorities and prevents generic open-web references from being introduced. GenIA-L does not apply human editorial validation to every individual generated respons. Final verification therefore remains the user's responsibility.	Noted
7.26	Can a response be generated without citations?	Yes. A response may be generated without citations where the task is based primarily on user-provided text, such as summarisation, extraction, comparison, drafting or reformatting, or where sufficiently relevant professional sources cannot be retrieved. For substantive legal, tax or accountancy research, the intended behaviour is to provide sources where available. The absence of citations should not be interpreted as evidence that an answer has been independently verified.	Noted
Model operation and auditing			
7.27	How does the system rank the importance of each section/chunk of a document? (Both user inputted and legal source documents)	Source documents and user-uploaded documents are segmented into passages or chunks that can be evaluated against the user's question. Chunks are ranked using semantic relevance and available document metadata. For uploaded documents, the platform extracts readable content and identifies prompt-relevant provisions such as clauses, dates, parties, obligations, risks or comparison points. The precise chunk size, overlap, treatment of tables and images, OCR process and ranking configuration are taking into account for the relevance ranking.	Noted
7.28	What is the context-window for a single prompt? (Including documents submitted alongside the prompt.)	The context capacity for a single request is governed by the production model configuration and includes the user prompt, active conversation context, retrieved passages and any extracted uploaded-document content. There is not a limit on the current maximum context window. Individual uploaded files are currently limited to 10 MB, but the file-size limit should not be interpreted as confirmation that every part of the file will fit within the model context.	Noted
7.29	What is the context-window for a single response?	The maximum generated response is controlled by the production output-token configuration. There is no limit set related to tokens generation. GenIA-L is designed to return a usable structured response within that limit. Users can ask follow-up questions, request additional detail or ask for the response to be divided into sections.	Noted

Ref	Requirement	Response	Reviewer Comments
7.30	What is the context-window for a continuous conversation?	GenIA-L maintains context across follow-up questions within the active conversation, subject to the model's total context capacity. There is not conversation limit. Users are instructed to start a New Chat when moving to a different client matter or topic. This prevents prior conversation or uploaded-document context from influencing the new matter.	Noted
7.31	What happens when the context window is reached or exceeded? (Including both the quality of answers and the warnings issued to end users)	GenIA-L does not impose a customer-facing token limit that users need to manage for standard prompt analysis or response generation. Context management is handled internally by the platform. The published limitation applies to uploaded documents, which must not exceed 10 MB or 150 pages per document. File size and page count are validated before analysis begins. If either limit is exceeded, the user is informed through an on-screen message and is asked to reduce, compress or divide the document before resubmitting it. An oversized document is not silently truncated or presented as having been analysed in full. Analysis does not proceed until the document complies with the applicable limits. This prevents an answer from being generated on the mistaken assumption that the complete document has been reviewed and avoids any related reduction in answer quality.	Noted
7.32	Can the system explain how a decision/output was reached, including the model's reasoning steps? How can the user view this and is there an audit trail that can be downloaded or viewed retrospectively?	GenIA-L provides source references and underlying excerpts that help the user understand and verify the basis of an answer. It does not expose private model chain-of-thought or hidden reasoning steps. Technical and security logs record operational metadata and relevant system events. Because customer prompts and outputs are not retained after the session, a complete historical prompt-and-response audit trail is not available for retrospective customer download.	Noted

Ref	Requirement	Response	Reviewer Comments
User workflow, prompting and accessibility			
7.33	Does the product provide structured prompting guidance/templates for common tasks?	Yes. GenIA-L provides prompting guidance and examples for common tasks. Guidance includes supplying relevant context, defining the objective, asking focused questions, specifying the desired output format and refining a request through follow-up questions. Document-analysis examples include summarising, extracting, reviewing, comparing and checking compliance. Users can also request structured outputs such as tables, checklists, FAQs or draft communications.	Noted
7.34	Can users annotate, compare, refine responses, and ask follow-up questions while maintaining context?	Users can compare documents or positions, refine an answer and ask follow-up questions while maintaining context within the active conversation. They can also request changes to structure, tone, scope or level of detail. GenIA-L does not currently provide a dedicated document-annotation or markup function. Users can copy or save the final output in their own systems and should start a New Chat when changing client matter or topic.	Confirmed
7.35	What accessibility features are currently supported (e.g., screen reader compatibility, keyboard-only navigation, colour contrast, text resizing/zoom, and captions/transcripts)? If any are not currently supported, what is the planned scope to address them and the target delivery dates?	GenIA-L has undergone an independent third-party accessibility assessment and is currently partially compliant with the European accessibility standard EN 301 549 version 3.2.1. The assessment methodology is based on EN 301 549 and incorporates the WCAG 2.2 Level A and AA success criteria. The audit was performed in February 2026 by an IAAP-certified accessibility specialist from Craftzing. The resulting accessibility statement was prepared on 4 March 2026. The audit found that GenIA-L met 58% of the applicable EN 301 549 criteria. The assessment covers accessibility requirements relevant to screen-reader compatibility, keyboard navigation, colour and contrast, text resizing and browser zoom, focus management, page structure and other assistive-technology interactions. As the product is only partially compliant, not all requirements in these areas are currently met. The identified non-conformities are recorded in the accessibility statement. The identified non-conformities will be addressed through a prioritised accessibility-remediation programme aligned with EN 301 549 and WCAG 2.2 Level A and AA.	Noted
7.36	Is the training limited to navigation, or does it also include guidance on query and prompt creation?	Training is not limited to navigation. It includes practical guidance on creating and refining prompts, providing context, specifying the intended objective and output format, using uploaded documents, interpreting source references and verifying AI-generated responses. Training also reinforces responsible use and the requirement for professional review.	Noted

Ref	Requirement	Response	Reviewer Comments
Document upload / attachments			
7.37	What file types (including documents and audio) can users upload or attach to queries, and what are the maximum file size numbers and limits?	GenIA-L currently supports PDF, DOCX, PPTX, JPG uploads and XLS, with a maximum size of 10 MB per document. Audio-file upload is not currently supported. Unsupported, oversized, corrupted, password-protected or unreadable files are rejected. Note that XLS files have just been re-added as an option, in response to customer feedback	Noted
7.38	Can customers configure or disable document retention settings?	No. Customers cannot configure or disable document-retention settings in the current version because uploaded documents are processed transiently and are not retained as persistent customer documents.	Noted
7.39	Are uploaded documents processed in full, partially extracted (e.g., text only), or transformed before being sent to any AI/LLM services?	Uploaded documents that comply with the applicable 10 MB and 150-page limits are validated and processed in full. Where a document contains machine-readable text, such as a text-based PDF or supported office document, its textual content is extracted directly without OCR. Where the document is image-based, such as a scanned PDF or an image file, OCR is performed first to convert the visible content into machine-readable text. OCR is used only as a necessary pre-processing step for documents that require text extraction; it is not applied to documents that already contain readable text. The extracted textual content, together with the user's prompt, is then provided for AI/LLM analysis. The document is not silently truncated or treated as fully analysed if its content cannot be successfully extracted. If the document is unsupported or unreadable, the user is informed before analysis proceeds.	Noted
7.40	Where are uploaded documents stored, how long are they retained?	Uploaded documents are held temporarily within the controlled EU/EEA-hosted service environment for the active request or session. They are encrypted in transit and during temporary processing and are automatically deleted when the session ends. They are not retained as persistent customer records or included in customer-content backups.	Noted
7.41	Who can access uploaded documents (end users, admins, support), and how is access logged/audited?	Uploaded documents are accessible to the authenticated user within the active request or session. Product administrators do not have routine access to uploaded files and do not receive direct storage access. Authorised technical or support staff may access only to operational metadata required to investigate service issues, subject to named accounts, RBAC, least privilege, MFA, monitoring and logging.	Noted

Ref	Requirement	Response	Reviewer Comments
7.42	What is the current roadmap for future enhancements document input / attachment functionality of the software (e.g. document management systems), with the expected scope and target timelines?	GenIA-L is not currently intended to operate as a full document-management system or general-purpose document repository. However, several enhancements to its document-input and attachment functionality are included in the 2026 product roadmap. The planned scope includes: - Increasing the maximum supported file size beyond the current 10 MB limit. - Supporting additional document types, including Excel files and spreadsheet analysis (now available since 24/7). - Improving the processing of large, scanned and image-based documents. - Introducing the Vault, a secure history capability intended to allow selected interactions and related content to be retained and revisited securely. These enhancements are targeted for delivery before the end of 2026. The scope and delivery dates remain indicative and are subject to technical validation, security and privacy assessment, accessibility review and controlled production deployment.	Noted
7.42 cont.		The Vault will require defined retention, encryption, tenant-segregation, access-control, deletion and data-residency arrangements before release. It is intended to provide secure product history functionality rather than replace customers' existing document-management systems.	
Hosting, UK market readiness & data residency transparency			
7.43	Are there UK paying customers for the tool today? If Yes: Confirm where production data is hosted, processed, and backed up, and from where the platform is administered and supported (including privileged access locations).	Yes. GenIA-L currently has paying UK customers. The production service is hosted on AWS infrastructure in the EU/EEA, with current materials referring to AWS European infrastructure, including Ireland. Identity services are provided through Azure AD B2C and LLM processing through OpenAI under a corporate arrangement that includes zero-data-retention controls. Customer prompts and uploaded documents are processed transiently rather than retained as customer records. Platform configuration, operational metadata, logs, account data and backups are maintained within the controlled AWS environment.	Noted
7.44	Are there paying customers for the tool outside of the UK? If Yes: Please provide a breakdown of key regions/countries served and confirm where customer data for those regions is hosted, processed, and backed up, including where the platform is administered and supported (including privileged access locations).	Yes. GenIA-L and related Lefebvre services are used by paying customers outside the UK, including customers in France, Belgium, Spain, Italy, the Netherlands, Germany and Luxembourg. The current architecture uses EU/EEA-hosted AWS infrastructure, Azure AD B2C for identity management and OpenAI for LLM processing under the group's approved contractual arrangements. Customer content is processed transiently and operational backups relate to platform and account data rather than retained prompts or uploaded documents. There aren't any differences in hosting, processing, backup or support arrangements by country, together with the countries from which privileged access occurs.	Noted

Ref	Requirement	Response	Reviewer Comments
Sub-processors, international transfers and contractual controls			
7.45	Which sub-processors process customer content (e.g. Hosting, LLM including prompts, uploaded documents, generated outputs) and which are 'corporate SaaS only'.	The principal subprocessors are: - AWS: hosting and infrastructure, including transient processing, platform storage, operational metadata and backups. - OpenAI: LLM processing of prompts, relevant retrieved passages, uploaded-document content where required and generated-output context. - Azure AD B2C: identity and authentication data; it does not ordinarily receive substantive prompt or document content. - PostHog: explicit in-product user feedback and associated product metadata. - Feedback may be triaged into Linear and operational alerts may be routed through Better Stack, Slack, SMS or telephone channels.	Noted
7.46	Where the vendor (or any of its sub-processors) processes or accesses UK customer personal data outside the UK (e.g., Australia or the USA), what international transfer mechanism(s) are relied upon to ensure UK GDPR compliance (e.g., UK IDTA or EU SCCs with the UK Addendum), and can you provide the relevant executed terms/templates on request?	GenIA-L is designed so that the primary hosting and processing of UK customer data takes place within the EU/EEA. The service uses AWS infrastructure located in Europe, including Ireland, and OpenAI services under a corporate agreement that includes zero-data-retention commitments and prohibits the use of customer data for model training. Where UK customer personal data is transferred to, processed in, or accessed from a country outside the UK/EEA, Lefebvre/Indicator applies the appropriate UK GDPR international-transfer safeguards. Depending on the transfer arrangement, these safeguards include the UK International Data Transfer Agreement (IDTA) or the European Commission's Standard Contractual Clauses supplemented by the UK International Data Transfer Addendum. These contractual safeguards are supported by the applicable transfer-risk assessments and supplementary technical and organisational measures, including encryption, access controls, least privilege, monitoring and restrictions on data retention and reuse.	Noted
7.46 cont.		The relevant executed transfer terms or applicable contractual templates can be provided to customers on request, subject to appropriate confidentiality arrangements or an NDA.. If any UK customer personal data is accessed or processed outside the UK/EEA by a vendor or staff member, the relevant transfer mechanism should be the organisation's UK GDPR-compliant mechanism, such as IDTA or EU SCCs plus UK Addendum.	Noted
7.47	How do customers access the current sub-processor list and receive notice of material changes (and is there an objection/termination right)?	Customers can request subprocessor information through normal due-diligence/support/account channels. The supplied materials identify the key current subprocessors but do not document the customer-facing notice, objection or termination process for material subprocessor changes.	Noted

Ref	Requirement	Response	Reviewer Comments
7.48	Do any sub-processors (or offshore staff) have access to customer environments for support/troubleshooting, and how is that access controlled and audited?	Subprocessor processing and staff access are limited to what is necessary to provide, maintain and support the service. Automated processing by AWS, Azure AD B2C and OpenAI is governed through the relevant service configuration and contractual arrangements. Administrative access is restricted through named accounts, RBAC, least privilege, MFA, monitoring and logging. Product administrators do not have routine access to uploaded documents or direct storage access.	Noted
AI/LLM usage, data use limitations and retention			
7.49	Is any customer data used for model training, tuning, evaluation, or product improvement? If yes, describe what is used, under what conditions, and can customers opt out?	Customer prompts, uploaded documents and generated outputs are not used to train, fine-tune or enrich Lefebvre/Indicator or third-party foundation models. Explicit feedback submitted through the in-product PostHog channel is reviewed by the R&D Team and may be triaged into the Linear development backlog. Quality-related feedback may trigger investigation and a new evaluation or improvement cycle, but is not used as model-training data.	Noted
7.50	What customer data is sent to the LLM provider (e.g., prompts, snippets, uploads, metadata), and what controls ensure it is not retained or reused beyond immediate processing?	OpenAI receives only the request information required for LLM processing: the user prompt, relevant retrieved source passages, applicable active-conversation context, uploaded-document content where required and the information needed to generate the response (Lefebvre/Indicator contents). Controls include the corporate OpenAI agreement, zero-data-retention arrangements, no use for model training or improvement, restricted service integration and transient processing. OpenAI's exact processing region (Europe), data retention measures for security or abuse monitoring, and the applicable endpoint configurations are guaranteed by the Group-level agreement that Lefebvre has signed with OpenAI.	Noted
7.51	How are user interactions (feedback, clicks, saved engagements, corrections) incorporated into the retrieval system (e.g., vector database)? And is this tenant-isolated?	User feedback is collected through a dedicated in-product PostHog channel. The R&D Team reviews feedback through PostHog dashboards and triages relevant items into the Linear backlog. Quality-related feedback triggers investigation and, if confirmed, enters the evaluation and improvement cycle; urgent matters follow the incident-management process. Customer prompts and generated responses are not retained in the retrieval index or used to train models. Feedback does not automatically modify the vector database.	Noted

Ref	Requirement	Response	Reviewer Comments
AI safety guardrails and responsible use			
7.52	Are prompts and responses logged to enable oversight and investigation of misuse?	Prompt and response content is not retained for general misuse oversight because of the zero-data-retention model. Oversight therefore relies on authentication and access logs, technical and security metadata, request controls, monitoring, anomalous-activity detection, user feedback and support escalation. This protects customer confidentiality but means that a complete historical reconstruction of prompt content is not normally available after the session.	Noted
7.53	What controls are in place to prevent, detect, or appropriately handle harmful, high-risk, or sensitive queries? Including those that could reasonably lead to unsafe or adverse outcomes if acted upon?	Controls include authentication and entitlement checks, operation within approved professional content sources, request and payload validation, file-type and malware controls, API gateway filtering, infrastructure and application monitoring, source presentation and responsible-use warnings. Queries outside the supported legal, tax or professional scope are not intended to receive authoritative advice. Users are reminded that GenIA-L supports rather than replaces professional judgement. Harmful, unsupported or out-of-scope queries should be handled through scope restrictions and responsible-use guidance	Noted
7.54	Can firms restrict usage to supported jurisdictions and domains (e.g., UK tax only), and does the tool warn users when queries fall outside supported scope?	Customers cannot currently configure a customer-admin toggle limiting all use to a particular jurisdiction or domain. . The tool is designed for legal/tax/professional domains and training materials state that it is not an open-web or general-purpose advice tool. Domain/jurisdiction restrictions are therefore controlled through the content corpus and entitlements, not through a customer-admin jurisdiction toggle	Noted
7.55	What measures minimise inaccurate citations or hallucinated authorities, and how are sources presented to support verification?	GenIA-L reduces the risk of hallucinated authorities and inaccurate citations by retrieving grounding material from the controlled Indicator/Lefebvre content corpus, presenting source references and enabling users to review the underlying content. Automated LLM-as-judge assessments are performed at regular intervals to identify response-quality degradation, including degradation following data or model changes. Confirmed degradation triggers investigation and a new evaluation and improvement cycle. User verification remains essential because these controls do not eliminate all citation or interpretation risk.	Noted

Ref	Requirement	Response	Reviewer Comments
Testing, errors and corrections			
7.56	What testing and quality assurance of the product has been performed specifically for the UK jurisdiction?	UK quality assurance includes editorial review of the Indicator UK content corpus, automated and manual evaluation of relevant tax and accountancy use cases, pre-production validation, multiple-reviewer approval and automated deployment gates. The product has also been positioned and tested for UK tax/accountancy use cases. Changes are first tested in isolation and then in an integrated pre-production environment. Production deployment is blocked if required evaluation or validation criteria are not met. Automated LLM-as-judge assessments monitor response quality between releases and over time.	Noted
7.57	Has the system been tested to the point of legal misinterpretation of the model due to reaching the limits of the context-window?	Context-limit risks are managed through prompt, payload and file-size controls, document processing and request validation. Users are encouraged to divide large matters into focused requests and verify the cited sources. The current evidence does not demonstrate that a specific stress test has been completed to identify the point at which context loss produces legal misinterpretation.	Noted
7.58	How are errors picked up by users tracked and remediated? Is there an escalation path for legally significant errors?	User-identified errors can be submitted through the in-product PostHog feedback channel or through support and account-management channels. The R&D Team reviews feedback in PostHog and triages confirmed issues into the Linear backlog. Quality-related errors enter the evaluation and improvement cycle. Urgent or legally significant issues follow the Incident Management Procedure and may result in investigation, root-cause analysis, an expedited hotfix, rollback to a known-good version or editorial-data re-indexing. All incidents are logged, investigated and documented. Post-incident reviews generate corrective and preventive actions, which are presented at the next Operational AI Committee meeting and tracked through the continuous improvement process.	Noted

Ref	Requirement	Response	Reviewer Comments
7.59	What per cent of queries have been marked as inaccurate by end users over the past: 3 months; 6 months; 12 months? (Or similar tracked periods.)	Based on the user-feedback data currently available, approximately 0.16 queries per 1,000 queries have been marked as inaccurate by end users. This is equivalent to 0.016%, or approximately one reported inaccurate response for every 6,250 queries. User feedback is collected through the in-product PostHog channel and reviewed by the R&D Team. Quality-related reports are investigated and, where confirmed, are added to the evaluation and improvement cycle or escalated through the incident-management process. The figure represents responses explicitly marked as inaccurate by users. It should not be interpreted as a statistically verified measure of the accuracy of all GenIA-L responses, because submitting feedback is voluntary and not every query is independently reviewed.	Noted
7.60	Does the system update users if something that has previously been generated is later found to be inaccurate?	GenIA-L does not currently retain prompt and output history, so it cannot automatically identify and notify every user who previously received a particular generated answer. Where an issue is connected to a support case, the affected customer can be contacted through that case. Broader or material issues may be communicated through product notices, account-management communications, updated documentation or other customer channels, depending on severity.	Noted
Reliability, transparency and user assurance			
7.61	Does the platform communicate limitations of AI-generated responses and encourage user verification where appropriate?	Yes. Product guidance communicates that GenIA-L is an AI-assisted professional research tool, is not guaranteed to be completely accurate and does not replace the judgement or responsibility of the professional user. Source references are provided where available so users can verify substantive answers against the underlying material before relying on them.	Noted
7.62	Does the platform outputs include confidence/quality indicators (e.g., source strength/recency), and how would users interpret them? If not, is this planned (with target release date)?	GenIA-L does not currently display a separate confidence or certainty score. User assurance is instead supported through source references, access to underlying material and responsible-use guidance. Automated LLM-as-judge assessments are used internally to monitor quality degradation but are not presented as user-facing confidence scores.	Noted
7.63	If confidence or quality indicators are provided, how are these generated (e.g. separate statistical model vs AI model output)? Can these be audited, explained, or validated by the user?	Not currently applicable. GenIA-L does not display a quantified confidence or certainty rating. Source selection and presentation are produced through the retrieval workflow rather than a separately disclosed confidence-rating model. Users can inspect the available sources but cannot audit a separate statistical confidence score because no such score is currently shown.	Noted

Ref	Requirement	Response	Reviewer Comments
7.64	Do sources/case treatments show reliability signals (e.g., positive/negative citing), and how would users interpret them? If not, is this planned (with target release date)?	GenIA-L presents references and underlying source content, but it does not currently claim to provide a comprehensive citator-style treatment signal showing positive, negative or neutral subsequent treatment of every case. Any reliability or treatment information available depends on the underlying professional content database.	Noted
7.65	Have the estimated certainty ratings been tested and shown to be stable over time? How is the stability measured?	Not applicable. GenIA-L does not currently display estimated certainty ratings, so no customer-facing certainty score is available for stability testing over time. Internal automated quality assessments monitor response-quality degradation between releases, but these should not be described as user-facing certainty ratings.	Noted
Authentication, access control and account security			
7.66	MFA is enforced for technical administrators. Please clarify the user roles available within the platform and whether if required by customers, MFA can be enabled for standard users and other privileged roles.	The current end-user model consists principally of named standard users who access conversational research and document-analysis functions according to their subscription entitlements. Technical and administrative roles are restricted to authorised Lefebvre/Indicator personnel. MFA is enforced for technical administrators. Customers using SSO can enforce MFA for their users through an OpenID Connect or SAML-compatible identity provider.	Noted
7.67	Can administrators enforce MFA for all users (and separately for privileged/admin roles)?	Customer administrators cannot currently enforce MFA from within a GenIA-L customer-admin settings screen based on the supplied materials. MFA is enforced for technical administrators. For standard users, MFA may be achievable via customer SSO/IdP policy where implemented. Confirm whether Azure AD B2C native MFA can be enabled platform-wide or per tenant for standard users.	Noted
7.68	Can customer administrators increase password requirements above the current enforced baseline (12 characters + uppercase letters, lowercase letters, alphanumeric characters, and special characters)?	No. Customer administrators cannot increase password requirements above the platform baseline from within the product. Current password policy is minimum 12 characters with uppercase, lowercase, alphanumeric and special characters. Customers using SSO may apply their own IdP password/MFA policies subject to supported integration.	Noted
7.69	Does the platform maintain a password history or prevent password reuse? If not, is there a roadmap to introduce password history and/or password reuse prevention? If so, will this be platform-wide or configurable by the customer?	GenIA-L-managed authentication does not currently maintain a customer-configurable password history or prevent reuse through a product-level setting. Customers using SSO may enforce password-history and reuse-prevention controls through their identity provider.	Noted

Ref	Requirement	Response	Reviewer Comments
Commercials, query limits and pricing mechanics			
7.70	Are research queries subject to any frequency, volume, concurrency, or fair-use limits by subscription tier, and how do these vary across plans?	GenIA-L does not currently apply a subscription-tier query allowance or per-query charge. However, technical request, file-size, payload, concurrency, rate and anti-abuse limits are applied to protect service availability and performance.	Noted
7.71	What happens if a customer exceeds limits (throttling, additional charges, plan upgrade), and how is usage measured and communicated to customers?	GenIA-L does not currently impose contractual, subscription-based or fair-use limits on the number, frequency or volume of research queries submitted by a customer. Customers are therefore not subject to throttling, additional usage charges or mandatory plan upgrades based on their query volume. Query usage is not presented to customers as a consumable allowance or quota and there is no customer-facing usage meter for billing purposes. Technical monitoring may measure service activity for operational performance, capacity planning and security purposes, but this information is not used to calculate additional charges. Separate technical limits apply to uploaded documents, which must not exceed 10 MB or 150 pages per document. If either limit is exceeded, the document is not processed and the user receives an on-screen message asking them to reduce, compress or divide the document before resubmitting it. Exceeding a document limit does not result in an additional charge or require a plan upgrade.	Noted

Ref	Requirement	Response	Reviewer Comments
Future plans and upgrades			
7.72	What future product developments or enhancements are planned? Please provide the expected scope, indicative timelines, and current roadmap status.	The current GenIA-L product roadmap includes continued development of the existing platform during 2026, followed by the planned introduction of a new platform during the first half of 2027. Planned developments during 2026 include: - Continued expansion and updating of the UK professional content corpus. - Development of the Vault, a secure history and content-management capability designed to preserve confidentiality and comply with applicable data-protection requirements. - Improvements to prompt processing, prompt interpretation and overall response quality. - Support for the analysis of Excel files and spreadsheet content. - Continued enhancement of retrieval, evaluation, monitoring and user functionality. The UK content expansion is ongoing. The Vault and the other identified product enhancements are currently in development or planned within the 2026 roadmap. Developments planned for Q1–Q2 2027 include the introduction of a new GenIA-L platform with.	Noted
7.72 cont.		The ability to search professional content from additional Lefebvre publishing businesses and content collections. User-profile personalisation, allowing the experience and responses to be better adapted to the user's professional context and preferences. Native voice-typing functionality. Enhanced and guided follow-up question functionality. A prompt library containing reusable prompts and examples for common professional tasks. Additional improvements to navigation, content discovery and the overall user experience. The Q1–Q2 2027 dates are indicative roadmap targets rather than contractual release commitments. Scope and delivery dates may be adjusted following technical assessment, user testing, security and privacy review, accessibility assessment and business prioritisation.	Noted
7.72 cont.		All new functionality is subject to Lefebvre/Indicator's documented AI system lifecycle, including risk assessment, evaluation, security and data-protection review, change management, pre-production validation and controlled production deployment.	Noted

Ref	Requirement	Response	Reviewer Comments
Other questions			
7.73	What output formats does the software support beyond text (e.g., tables, charts, diagrams, flowcharts, or other visualisations)?	GenIA-L principally produces text-based responses. It can generate structured outputs such as tables, summaries, comparisons, checklists, FAQs, draft emails or letters, and text-based flowcharts or decision trees. It does not currently provide a dedicated native charting or graphical-visualisation engine. Structured text and tables can be copied into office or visualisation tools for further formatting.	Noted
7.74	Does the software support voice dictation for inputs?	GenIA-L does not currently provide native voice-dictation or audio-input functionality. Users may use compatible operating-system or browser dictation tools to enter text, subject to their own device, browser, accessibility and security settings.	Noted