Overview

Supplier	Recite Me Limited
Hellios ID:	10029554
Published Date	18/08/2026
Questionnaire Status	Complete
Renewal Date	25/08/2027
Questionnaire Version	13.0

Registration Contact Details

First Name	Simon
Last Name	Backwell
Job Title	Information Security and Data Protection Officer
Email Address	simon.backwell@reciteme.com
Telephone Number	
Mobile Number	

Questionnaire

1.1 Company Contact

1.1.1 Full Company Name
Recite Me Limited

1.1.2 Does your company use any other trading names?
No

1.1.3 Company Address

1.1.4 Address Line 1
Baltimore House

1.1.5 Address Line 2 *(optional)*
Baltic Business Quarter

1.1.6 Address Line 3 *(optional)*

1.1.7 Town/City
Gateshead

1.1.8 Postcode/Zipcode
NE8 3DF

1.1.9 Country

United Kingdom

1.1.10 County/State *(optional)*
Tyne and Wear

1.1.11 Company Main Telephone Country Code *(optional)*
United Kingdom +44

1.1.12 Company Main Telephone Number *(optional)*
1914328092

1.1.13.0 Does your company have a website?
Yes

1.1.13 Company Website Address
https://reciteme.com/

1.1.14 Please select the following regional locations where your company has a physical office or depot.
North England

1.1.15 Please select the following global locations where your company has a physical office or depot.
Australia
United Kingdom
United States of America

1.1.16 Is your company a current customer of Lloyds Banking Group?
Yes

1.1.17 Please select the following global locations from which your organisation provides products or services.
Australia
United Kingdom
United States of America

1.3 Financial & Legal

1.3.1 Do you have a legal Company Registration Number?
Yes

1.3.1.1 Company Registration Number
07258145

1.3.1.4 Is your company VAT registered?
Yes

1.3.1.2 Company VAT Number
GB114648030

1.3.1.3 Country of Registration
United Kingdom

1.3.2 Please enter your 9 digit D-U-N-S number.
216736922

1.3.3 Year Company Founded
2010

1.3.4 Company Ownership Structure
Private Limited

1.3.5 Company Latest Published Annual Revenue
6005082

1.3.5.1 Company Annual Revenue Currency
GBP

1.3.5.2 Company Annual Revenue Year End
31 03 2025

1.3.6 Number of Total Employees?
71

1.3.7 Is your company a subsidiary of another company?
No

1.3.7.6 Is your company a Parent of another company?
No

1.3.8 Please confirm that your company holds the following valid insurance policies.
Yes - Cyber Liability
Yes - Employers Liability
Yes - Products Liability
Yes - Professional Indemnity
Yes - Public Liability

1.3.9 Does your company have a LEI (Legal Entity Identifier) code?
No

1.3.10 Does your company have an EUID (European Unique Identifier)?
No

1.3.11 Is your company publicly listed on any stock exchanges?
No

1.4 Product & Service Supply

1.4.1 Please select the products or services that your Company wishes to provide
0523 - Software Development - Corporate
0525 - Software Development - Enterprise
0537 - Software Development - Digital
0554 - Software Consultancy

1.4.2 Please select the locations that you are able to supply these products or services to
Africa
Asia
Australasia
Europe
Global
Ireland
Middle East
North America
South America
UK

1.4.4 Are any of the products or services selected regulated by an official regulator?
No

1.4.5 Is your company covered by an officially recognised third-party certification, for example ISO certificates or other accreditations?
Yes

1.4.5.1 Please select which third-party certifications:
Cyber Essentials
Cyber Essentials Plus

1.5 Customer Treatment

1.5.1 Will your company be in contact with your client's customers or employees on behalf of your clients, either directly or indirectly through supporting a service provided by another company?
No

1.5.2 Will any service your company provides to your clients involve an actual or potential commission payment being made?
No

1.5.3 Will your company design and/or manufacture financial services products that are sold by you, your client or a third party, and could be used by your client's customers?
No

1.5.4 Will your company offer financial services directly to your client's customers or employees on their behalf?
No

1.5.5 Will your company be supplying information and advice to your client's customers on their behalf either verbally or via a durable medium?
No

1.5.6 Will there be a requirement for your company to segregate your client's customer payments or assets from your own?
No

1.5.7 Will your company handle complaints for your clients, including receiving and reviewing complaints on their behalf, or handle complaints related to your own services for their customers?
No

1.5.8 Will you be providing a critical component of payment services on your client's behalf?
This includes, but is not limited to:
1. Instructing a payment on behalf of the client or their customers
2. Processing a payment on behalf of the client either through using their systems or your own IT systems
3. Providing a Payment Initiation Service and/or Account Information Service on behalf of the client
4. Managing or reconciling Accounts that are used for payments execution
5. Monitoring Payments Data on behalf of the client
6. Processing any financial transaction on behalf of the client, such as receipts.
No

1.5.9 Does your company sell products on behalf of any other organisation?
No

1.5.10 Does your company undertake market or product research on behalf of your clients?
No

1.5.11 Does your company undertake debt collections services on behalf of any other organisation?
No

1.6 Security

1.6.1 What level of access will your company or employees require to your client's systems, network or data to provide its products or services?
No access

1.6.2 What level of access will your company or employees require to your client's physical assets and/or premises to provide products/services?
No access

1.6.2.1 What level of access will your company or employees require to your client's customers' physical assets and/or premises to provide products/services?
No access

1.6.3 Will your company be hosting any IT systems or data on your client's behalf either directly or through any affiliated or subcontracted party?
No

1.6.4 Will your company or any subcontractor store, transfer, process, handle or have access to any of your client's data that is not in the public domain?
No

1.6.5 Will your company or any subcontractor be capturing, creating, managing, storing and/or destroying any client-owned records?
No

1.6.6 Will your company or any subcontractor be collecting and/or processing personal data?
Yes

1.6.23 Will your company or any subcontractor be collecting and/or processing non-personal data?
Yes

1.6.10 Will you be supporting your clients in the provision of staff or on-site services?
No

1.6.11 Will you be involved with the disclosure and/or dissemination of your client's information to the Markets as a result of your client's listed debt or equity?
No

1.6.12 Is your company required to either comply with the prevailing Money Laundering Regulations or will be providing services that constitute part of your client's anti-money laundering control framework?
No

1.6.13 Does your company or any subcontractors provide products and services that directly assist your clients in meeting any of the following customer asset management schemes?
No

1.6.15 Does your company or any subcontractor manage any systems, controls, processes, network and data for your clients or have access that could have a fraud impact on your client or your client's customers?
No

1.6.18 Will your company be providing any technology products and services for your clients?
Yes - COTS technology not hosted on client premises

1.6.20 Does your company transmit, store, dispose or handle credit/debit card data for or on behalf of your client?
No

1.6.21 Will your company or any subcontractor store, transfer, process or handle any of your client's physical assets or financial assets?
No

1.6.22 Will your company deliver changes to your IT systems and/or processes on behalf of and/or impacting your client?
No

1.7 Responsible Business

1.7.1 Please select the countries where your company has or does any of the following:
- An office or other physical presence
- A relationship with a local company, government or other organisation
- Process payments or undertake commercial transactions

Australia
United Kingdom
United States of America

1.7.5 Will your company be either acting on behalf of or representing in the name of your clients?
No

1.7.6 All organisations operating or doing business in the UK are required to comply with the Modern Slavery Act 2015. If you are unclear about what your obligations are under the Act please click [HERE|https://www.gov.uk/government/publications/transparency-in-supply-chains-a-practical-guide] -link to the MSA 2015 and the Government guidance

1.7.6.0 Is your company required to publish a Modern Slavery Statement on your website?
No

1.7.6.7.0 Has your company published a Modern Slavery Statement on your website within six months of your most recent completed financial accounts?
No

1.7.7 Does your company have a written policy and procedure(s) for managing compliance with Part 3 of the Criminal Finances Act 2017 and/or any equivalent facilitation of tax evasion legislation or regulation in other jurisdictions in which your company operates?
No

1.7.8 Is your company a social enterprise?
No

1.7.9 Does your company have a Net Zero commitment by 2050 or sooner?
No

1.7.10 Is your company a certified B-Corp?
No

1.7.11 Does your company have policies and procedures in place to ensure compliance with the relevant laws and regulations for the products and services you provide?
Yes

1.7.12 Does your company have the required business licences, consents, approvals, registrations and notifications in the applicable jurisdictions in which your company operates?
Yes

1.8 Business Continuity

1.8.2 Do any of the systems or services you supply your clients have to be available in less than 24 hours?
Yes (recovery time < 24 hours)

1.8.3 Do you currently use, or plan to use, any third party (e.g. subcontractors or outsourced providers) to deliver any part of the service you provide to your clients?
Yes

1.9 Policy Compliance

1.9.1 Please confirm you have read, understood and will comply with Lloyds Banking Group's Health, Safety & Fire Policy Summary for Third Party Suppliers https://www.lloydsbankinggroup.com/who-we-are/working-with-suppliers/policy-compliance.html.
Yes

1.9.2 Please confirm you have read, understood and will comply with Lloyds Banking Group's Compliance Policy for Third Party Suppliers https://www.lloydsbankinggroup.com/who-we-are/working-with-suppliers/policy-compliance.html.
Yes

1.9.3 Please confirm you have read, understood and will comply with Lloyds Banking Group's Code of Supplier Responsibility https://www.lloydsbankinggroup.com/who-we-are/working-with-suppliers/policy-compliance.html.
Yes

1.9.5 Please confirm you have read, understood and will comply with Intact Insurance's Code of Conduct https://www.rsagroup.com/media/m1xixndz/rsa-supplier-code-of-conduct-2022.pdf.

1.9.7 Please confirm you have read, understood and will comply with Nationwide's Third Party Code of Practice https://www.nationwide.co.uk/suppliers/policies#tab:Policies

1.9.8 Please confirm that you have read, understood and comply with the Bank of Ireland's Code of Supplier Responsibility https://hellios.com/hubfs/Products/fsqs/BOI-Code-Of-Supplier-Responsibility-November-2025.pdf.

1.9.9 Please confirm you have read, understood and will comply with Lloyds Banking Group's Anti-Bribery Policy https://www.lloydsbankinggroup.com/who-we-are/working-with-suppliers/policy-compliance.html.
Yes

1.9.10 Please confirm you have read, understood and will comply with Santander's Code of Supplier Responsibility https://www.santander.co.uk/about-santander/our-business/suppliers/compliance.

1.9.12 Please confirm you have read, understood and will comply with FirstRand's Supplier Code of Conduct https://hellios.com/hubfs/Products/fsqs/FirstRand-Supplier-code-of-conduct-Mar-2026.pdf.

1.9.13 Please confirm you have read, understood, and will comply with Bank of England's Supplier Code of Practice https://www.bankofengland.co.uk/-/media/boe/files/about/supplier-code-of-practice.pdf?

la=en&hash=F5B3DB8FE1579A0D30430DFA474F262BE53C3A6E

1.9.14 Please confirm you have read, understood and will comply with ABN AMRO Bank's Code of Conduct https://hellios.com/hubfs/Products/fsqs/241209_ABNAMRO_Supplier_Code_of_Conduct_Jan2026.pdf.

1.9.15 Please confirm you have read, understood, and will comply with Metro Bank's Supplier Code of Conduct http://hellios.com/wp-content/uploads/2022/09/MB-supplier-code-of-conduct-compressed_1-1.pdf.

1.9.16 Please confirm you have read, understood, and will comply with the FCA Supplier Code of Conduct https://www.fca.org.uk/publication/corporate/supplier-code-of-conduct.pdf.

1.9.17 Please confirm you have read, understood and will comply with Lloyds Banking Group's Speak Up Third Party Policy https://www.lloydsbankinggroup.com/who-we-are/working-with-suppliers/policy-compliance.html.
Yes

1.9.18 Please confirm you have read, understood and will comply with PTSB's Sustainable Supplier Charter https://www.permanenttsb.ie/responsible-business/Suppliers/suppliers/.

1.9.19 Please confirm you have read, understood, and will comply with the Arbuthnot Latham Supplier Code of Conduct https://www.arbuthnotlatham.co.uk/important-information.

1.9.20 Please confirm you have read, understood and will comply with Bank of Ireland's Third Party Policies https://hellios.com/hubfs/Products/fsqs/BOI-Third-Party-Policies-November-2025.pdf.

1.9.21 Please confirm you have read, understood and will comply with TSB's Responsible Supplier Charter https://www.tsb.co.uk/tsb-responsible-supplier-charter/.

1.9.22 Please confirm you have read, understood and will comply with esure's Supplier Code of Conduct https://hellios.com/wp-content/uploads/2024/06/supplier-code-of-conduct-1.pdf.

1.9.23 Please confirm that you have read, understood and will comply with the Redwood Bank Supplier Code of Conduct https://redwoodbank.co.uk/inside-redwood/supplier/.

1.9.24 Please confirm that you have read, and understood the Redwood Bank Modern Slavery Statement https://redwoodbank.co.uk/legal/2023-modern-slavery-statement/.

1.9.25 Please confirm that you have read, understood and will comply with Fidelity International's Supplier Code of Conduct https://hellios.com/hubfs/Products/fsqs/fidelity-supplier-code-of-conduct-june-2025.pdf.

1.9.26 Please confirm that you have read, understood and will comply with the NFU Mutual Supplier Relationship Code https://indd.adobe.com/view/afc75117-4db7-4984-9bc7-cef0db4f5d66.

1.9.27 Please confirm that you have read, understood and will comply with West Brom Building Society's Supplier Code of Conduct https://www.westbrom.co.uk/suppliers/supplier-code-of-conduct.

1.9.28 Please confirm that you have read, understood and will comply with Benefact Group's Supplier Code of Conduct https://hellios.com/hubfs/Products/fsqs/benefact-group-supplier-code-of-conduct-dec2025.pdf.

1.9.29 Please confirm that you have read, understood and will comply with Family Building Society's Supplier Code of Conduct https://hellios.com/hubfs/Products/fsqs/family-building-society-supplier-code-of-conduct-feb-26.pdf.

1.9.30 Please confirm that you have read, understood and will comply with Wesleyan's Supplier Charter https://www.wesleyan.co.uk/docs/default-source/pdf/wesleyan-third-party-suppliers-charter.pdf.

1.9.31 Please confirm that you have read, understood and will comply with Newbury Building Society's Supplier Code of Conduct https://hellios.com/hubfs/Products/fsqs/Newbury-Building-Society-Supplier-Code-of-Conduct-Mar2026.pdf.
Yes

1.9.32 Please confirm that you have read, understood and will comply with Irwin Mitchell's Supplier Code of Conduct https://hellios.com/hubfs/Products/fsqs/Irwin-Mitchell-Supplier-Code-of-Conduct-July2026.pdf.

1.10 Declaration

1.10.1 Has your company previously been or is currently involved in a legal dispute and/or sanctions violation related to financial sanctions imposed by the United Nations, European Union, HM Treasury, US Office of Foreign Assets Control, or other competent authority in the past 10 years?
No

1.10.2 Has your company previously been, or is currently, involved in a legal dispute related to Anti Money Laundering regulation in the past 10 years?
No

1.10.3 Has your company had any reportable Health & Safety accidents, incidents or fatalities in the past 12 months?
No

1.10.20 Has your company or any of its subcontractors experienced any work-related fatalities in the last five years?
No

1.10.4 Has your company or any of your officers, employees or beneficial owners been convicted of any offence under the UK Bribery Act 2010, US Foreign Corrupt Practices Act or equivalent legislation in any other jurisdiction in the past 10 years?
No

1.10.5 Has your company or any of your officers, employees, or beneficial owners been convicted of any offence under the UK Criminal Finances Act or equivalent legislation in any other jurisdiction in the past 10 years?
No

1.10.6 Has your company or any director of your company been declared bankrupt or insolvent in the past 3 years?

No

1.10.7 Has your company been fined by any regulatory bodies or governing bodies due to violations or non-compliance in the past 10 years?
No

1.10.8 Has your company or any of its directors been the subject of any criminal or civil court action in respect of your company's business activities in the past 3 years?
No

1.10.9 Is your company government or state linked?
No

1.10.10 Is your company under investigation or currently subject to any supervisory or enforcement actions by any regulatory or governing bodies?
No

1.10.11 Has your company been the victim of any reportable cyber security events in the last 12 months?
No

1.10.12 Has your company been the victim of any reportable data breach events in the last 12 months?
No

1.10.13 Has your company been served with a Prohibition or Improvement Notice, or been prosecuted for any breaches of Health & Safety legislation in the last five years?
No

1.10.14 Please confirm that your company, any director/partner, or anyone directly involved in the provision of your products/services has not been subject to regulatory action or legal proceedings as a result of alleged tax evasion or facilitation of tax evasion in any jurisdiction?
Yes - we confirm there has been no regulatory or legal actions for tax evasion

1.10.15 Have there been any physical security incidents (i.e. theft, burglary) at any location where customers are being served from in the last five years?
No

1.10.17 Have any material findings been identified in relation to your company as a result of an internal audit or an independent review (e.g. by an external auditor, independent third party, regulator, or government body) in the last two years?
No

1.10.18 Has your company been subject to any legal or regulatory proceedings relating to the processing of personal or corporate data in the last five years?
No

1.10.19 Has your company been subject to any material data breaches or similar incidents that adversely affected the confidentiality, integrity, or availability of data in the last five years?
No

1.12 US Tariffs

One of the fundamental guiding principles of FSQS is to avoid duplication of requests. In response to President Trump's Executive Order on Reciprocal Tariffs (2nd April 2025) the financial services firms using FSQS need to understand any potential implications on their supply chains including any resilience concerns and impacts of broader macroeconomic effects resulting directly or indirectly from the tariffs and other related no tariff trade barriers. FSQS buyer members have agreed to use FSQS to gather the information needed from suppliers and minimise the need for separate requests for information. This coordinated approach is expected to save the industry a significant amount of time and effort.[br][br]We ask that you complete the questions in this section with urgency and then review and update any answers should your organisation's position change in the future.

1.12.1 Is your organisation impacted by the tariffs imposed in the President's Executive Order on Reciprocal Tariffs (2nd April 2025)?
No

1.11 Terms & Conditions

1.11.1 Please confirm you have read and understood the Hellios terms and conditions of registration https://hellios.com/hubfs/Products/fsqs/Hellios-FSQS-Supplier-Terms-and-Conditions-v5.2.pdf.
Yes

2.1 Anti-Bribery

2.1.1 Does your company have a written policy and procedure(s) for managing compliance with the UK Bribery Act 2010 and any equivalent Anti-Bribery legislation or regulation in other jurisdictions in which your company operates?
Yes – Not Willing to Upload Document

2.1.2 Does your anti-bribery process include the following:

2.1.2.1 Regular risk assessments to identify and mitigate inherent risk?
Yes

2.1.2.2 Regular training for all employees covering Anti-Bribery and Corruption, including upon induction?
Yes

2.1.2.3 Regular internal audit review, including external audit review where appropriate?
Yes

2.1.2.4 Detailed Root Cause Analysis (RCA) upon detection of a bribery and corruption event?
Yes

2.1.2.5 Key anti-bribery metrics and KPIs reported to internal committees/Senior Management?
Yes

2.1.2.6 Controls in place to inform your client if you breach anti-bribery regulatory requirements?
Yes

2.1.2.8 Controls to detect and prevent facilitation payments being made?
Yes

2.1.2.9 Escalation and reporting methods if a facilitation payment is made?
Yes

2.1.2.7 How many months are there between reviews of your Anti-Bribery Policy?
12

2.1.3 Is a senior manager or board member responsible for setting the 'tone from the top' with regards to communications policy around anti-bribery?
Yes

2.10.0 Does your company have a written policy and/or documented procedure(s) for Conflicts of Interest?
No

2.10.2 Does your company identify and maintain a record of gifts, entertainment and hospitality either offered or received?
Yes - Offered & Received

2.10.2.2 Does your company provide training to maintain awareness of a gifts, entertainment and hospitality record?
No

2.10.2.3 Does your company report MI including breaches of your gifts, entertainment and hospitality record to Senior Management?
No

2.10.3 Does your company have a Market Abuse Policy that includes controls to prevent insider-dealing, market manipulation and other activities covered by the Market Abuse Regulation that may impact market integrity?
No

2.3 Operational Risk

2.3.1 Does your company have a documented process to identify any operational risks across your products/services, activities, people, processes and systems that could impact your client's customers or reputation?
Yes – Willing to Upload Document

2.3.1.1 Please upload your operational risk process.
Risk Management Procedure.pdf

2.3.1.2 Has your operational risk process been approved by senior management and/or the board?
Yes

2.3.1.3 Has your operational risk process been communicated to all relevant stakeholders?
Yes

2.3.1.4 Please give the date of your last review of your operational risk process.
04 08 2025

2.3.2 Does your operational risk process include the following:

2.3.2.1 Regular assessments to identify where risks may not be sufficiently mitigated?
Yes

2.3.2.2 Regular review and maintenance of risk records?
Yes

2.3.2.3 Controls to ensuring continual compliance with any SLAs with your clients?
Yes

2.3.2.4 Identifying, assessing, and testing the key controls to mitigate the risks?
Yes

2.3.2.7 Identifying and escalating operational risk events?
Yes - material and other events

2.3.2.9 A requirement to regularly produce and share Risk and Control Management Information to board level or equivalent within your company?
Yes

2.3.2.10 A requirement to advise clients of an event / incident within 24 hours?
Yes < 24 hours

2.3.2.11 Root Cause Analysis, mitigating similar issues in future and reporting of outputs, including details of remedial and preventative actions taken shared with clients that have been impacted?
Yes

2.3.3 Does your company apply a baseline set of minimum controls that need to be configured on all End User Computing Application's (EUCA's), to ensure adequate governance over its use and protection of the data that is contained within it?
Yes

2.12 Health & Safety

2.12.0 Does your company have a documented Health & Safety Policy?
Yes – Not Willing to Upload Document

2.12.2 Does your Health & Safety Policy include the following:

2.12.2.2 Regular training for all employees on this policy including upon induction?
Yes

2.12.2.4 Details of the arrangements in place for monitoring Health & Safety performance?
No

2.12.2.5 Details of recording and reporting of Health & Safety accidents and incidents, either internal or external?
Yes

2.12.2.6 A requirement to incorporate the needs of vulnerable people?
No

2.12.2.7 The requirement to conduct risk assessments for all work activities across all office locations?
Yes

2.12.2.8 Emergency arrangements for buildings with designated roles and responsibilities?
Yes

2.12.2.9 Pre-work procedures, including permit to work requirements?
Yes

2.12.2.10 Guidelines for cessation of work?
Yes

2.12.2.11 Standard operating procedures for the use of heavy machinery, tools, and vehicles?
No

2.12.2.12 Food hygiene and safety procedures?
No

2.12.3 Is a senior manager or board member responsible for your Health & Safety Policy?
Yes

2.12.13 Does your company have processes in place relating to supporting the mental health and well-being of employees in the workplace?
Yes

2.12.14 Does your company ensure that all employees and subcontractors receive health & safety training relevant to their job description?

No

2.12.15 How does your company ensure health & safety requirements are communicated and understood by your employees?
Intranet
Notice board or other internal communication

2.13 Whistleblowing

1.7.2 Does your company have a Whistleblowing policy or training material that enables any employee to freely report any perceived issues that might impact your clients or their customers?
Yes – Willing to Upload Document

2.13.1 Please upload your whistleblowing policy and process.
Whistleblower Policy - Jan 25.pdf

2.13.1.1 Please give the date of the last review of your whistleblowing policy.
12 01 2025

2.13.2 Does your whistleblowing policy include the following:

2.13.2.1 Training on this process at least annually for all existing staff and for all new staff upon induction?
Yes

2.13.2.3 Controls to ensure that any allegations impacting your client's employees, their customers or your clients as a whole are reported to your clients?
Yes - Internal Monitoring

2.13.2.4.1 The requirement that all concerns must be dealt with confidentially?
Yes

2.13.2.5 Detailed root cause analysis upon detection of a whistleblowing event?
Yes

2.13.2.10 Examples of wrongdoing?
Yes

2.13.2.11 Protection for individuals reporting a concern, resulting in formal action in the event of harassment or victimisation?
Yes

2.13.2.12 A statement that individuals should not be prevented from reporting a concern?
Yes

2.13.2.13 Formal action against the relevant management in the event that any reported concerns are not acted upon?
Yes

2.13.2.16 Ability for employees, contractors, temporary workers, and third parties to report concerns anonymously?
Yes

2.13.4 Has your company had any Whistleblowing cases that have impacted any of your clients?
No

2.14 Human Resources

2.14.14 Does your company train employees on organisational culture and values?
Yes

2.14.15 Do senior management regularly communicate your organisation's culture and values to employees?
Yes

2.15 Physical & People Security

2.15.1 Does your company formally review the physical security environment and risks at least annually and whenever there is a significant change in risk to your clients?
Yes

2.15.1.1 Please give the date of your last documented review.
01 07 2026

2.15.2 Does your company have measures in place to prevent and detect the unauthorised removal of systems and devices that store or process your client's data?
Yes

2.15.3 Is access to your company's premises prevented from unauthorised access by electronic-controlled access doors or barriers?
Yes

2.15.3.2 Is access specifically controlled and monitored to any room or area where your client's data is being stored or processed?
Yes

2.15.3.3 Does your company have the facility to segregate physical space, resources and data by client?
No

2.15.4 Is your company's premises protected by CCTV 24 hours a day?
Yes

2.15.4.0 What is the minimum period of time your CCTV footage held for?
More than 28 days

2.15.4.2 Is all CCTV footage held for a minimum of 90 days for any high risk or regulated areas?
Yes

2.15.5 Are all visitors to your company's premises recorded and issued a visitor pass?
Yes

2.15.5.1 Are all unvetted visitors to your premises escorted by a company employee?
Yes

2.15.6 Is your company's premises protected by physical intrusion detection systems?
Yes

2.15.7 Are your company's electronic security systems maintained and monitored by an industry-recognised security company?
Yes

2.15.8 Does your company have a named person who is responsible for physical security?

Yes

2.15.9 Does your company ensure that personnel, including contractors and third parties, have signed relevant Confidentiality or Non-Disclosure Agreements (NDAs) where applicable?
Yes

2.15.10 Do your company's premises and IT services have a UPS system and back-up power generator installed?
Yes

2.15.10.1 Are the UPS systems and generators tested at least annually?
Yes

2.15.11 Does your company periodically conduct physical security training and awareness programmes for all employees and contractors who will have access to client assets or data?
Yes

2.15.11.1 Does the training include security drills and evacuation exercises?
Yes

2.15.12 Does your company have environmental controls in place in all areas where customer assets are stored and/or managed?
Yes

2.15.13 Do the environmental controls include the following:

2.15.13.1 Buildings equipped with fire detection, alarming and suppression systems (e.g. automatic water sprinklers, gas detectors, manual extinguishers, fire alarms) that are periodically tested?
Yes

2.15.13.2 Electrical power supplied through a Uninterruptible Power Supply (UPS) system that is periodically tested, with security systems (e.g. access control, alarms) connected to the building's UPS system?
Yes

2.15.14 Does your company have security and surveillance controls in place at all facilities where customer assets are stored and/or managed?
Yes

2.15.15 Do the security and surveillance controls include the following:

2.15.15.1 Intrusion detection and alert systems installed on accessible external doors and windows at the buildings or data centres?
Yes

2.15.15.2 Security video surveillance installed in strategic areas, which are recorded and monitored with images retained for a minimum of 30 days?
Yes

2.15.15.3 Security guards positioned to respond to a security-related incident?
Yes

2.15.16 Does your company perform any physical security control audits?
Yes

2.15.16.1 Were there any issues identified during the latest physical security audit that are subject to remedial action?

No issues noted in audit report

2.15.17 Do the physical security control audits include the following:

2.15.17.1 Full inventory audits of the high value assets that your company holds for your clients?
Yes

2.15.17.2 Independent security assessment by a regulatory body or insurance company?
No

2.15.18 If the buildings used by your company in the supply of products and services to your clients were unavailable, would this impair your ability to fulfil your contractual obligations, and where defined, meet agreed SLAs?
No

2.15.19 Does your company complete regular maintenance of building(s), including structure, rooftops, signages, facades, and electrical and mechanical equipment, in accordance with legal requirements?
Yes

2.15.20 Does your company regularly test the response to the loss of a utility (e.g. electricity), or the loss of a part of the infrastructure?
Yes

2.15.21 Does your company ensure that all applicable building permits and licences required are in place and renewed in a timely manner?
Yes

2.15.22 Does your company have a physical security breach response procedure?
Yes

2.15.23 Does your company have a documented asset addition/removal process which ensures any of your client's assets movement instructions are appropriately authorised?
Yes

2.15.24 Does your company have policies, standards, or procedures for physical security and site security assessment in order to protect customer assets within your environment/ premises?
Yes

2.15.24.1 Have these policies, standards, or procedures been reviewed and approved by management in the last 12 months?
Yes

2.15.25 Do these policies, standards, or procedures include the following:

2.15.25.1 Site security assessments carried out on a defined frequency and in response to a trigger event?
Yes

2.15.25.2 Are site security assessments presented to your customer upon request?
No

2.15.25.3 Communication of this policy to all employees (including contractors and part-time) through training awareness programmes, other publications, and/or intranet?
Yes

2.15.26 Does your company have documented procedures for physical access control?
Yes

2.15.27 Do your company's physical access control procedures include the following:

2.15.27.1 Controlling physical access to buildings or data centres at entrance points (e.g., by the use of a badge, access card, biometrics, turnstile entry door, security guards etc)?
Yes

2.15.27.2 Physical access provisioning, revocation and access recertification executed in a timely manner, with access logs maintained (both for employees and visitors)?
Yes

2.15.27.3 Restricting access to areas of the building containing customer assets or information (e.g., server room, storage facility, vault) to authorised personnel only?
Yes

2.15.27.4 Ballistic and/or blast resistant features and adequate perimeter protection where applicable (e.g., penetration resistant anti-climb walls)?
Yes

2.15.27.5 All venting/air-conditioning intakes protected against intrusion where applicable?
Yes

2.15.27.6 Adequate procedures and controls for key holding, key replication, and PIN codes for critical areas?
Yes

2.15.27.7 Segregated ingress/egress points installed for multi-tenant environments?
Yes

2.15.27.8 Requirement for physical segregation and securing of IT equipment in multi-tenant data centres?
Yes

2.15.27.9 Conducting of independent site penetration tests, and sharing the reports with customers upon request?
Yes

2.15.28 In the event of physical security incident, how long does it take your company to notify your clients?
Within 8-24 hours

2.16 Fraud

2.16.1 Are pre-employment vetting checks undertaken for all employees?
Yes

2.16.2 Does this vetting process include the following checks for each employee:

2.16.2.1 Name, address and telephone number?
Yes

2.16.2.2 Right to work documentation (verified according to Home Office guidelines)?
Yes

2.16.2.4 Credit checks?
No

2.16.2.5 Criminal Background checks?
Yes

2.16.2.7 Sanctions check?
No

2.16.2.12 CIFAS checks, or equivalent local fraud database checks?
No

2.16.2.11 Politically Exposed Person checks?
No

2.16.2.9 References covering at least the last three years?
Yes

2.16.2.13 Identity verification?
Yes

2.16.2.17 Professional Qualification and Membership checks where required for the role?
Yes

2.16.2.18 Insurance Fraud Register (IFR) checks?
Yes

2.16.2.19 Public media (negative news) checks?
No

2.16.2.20 Education checks?
Yes

2.16.2.21 Required qualifications checks?
Yes

2.16.2.22 Employment history checks?
Yes

2.16.10 Are any of your employees on the Insurance Fraud Register (IFR)?
No

2.17 Business Continuity & Disaster Recovery

2.17.0 Does your company have a policy that documents your approach to Business Continuity and Crisis Incident Management?
Yes – Not Willing to Upload Document

2.17.0.2 Does your company's policy that documents your approach to Business Continuity and Crisis Incident Management include the following:

2.17.0.2.1 Accountabilities and responsibilities for incident response based on clearly defined roles?
Yes

2.17.0.2.2 Training on this process at least annually for staff who have business continuity responsibilities?
Yes

2.17.0.2.6 Training on this process at least annually for staff who have incident response responsibilities?
Yes

2.17.0.2.3 Notification to your clients on any incidents impacting services provided?
Yes

2.17.0.2.4 Processes/plans in place for responding to incidents which impact the service?
Yes

2.17.0.2.5 Contingency plans in place to notify clients in the event of an outage or any disruption?
Yes

2.17.0.2.7 Accountabilities and responsibilities for Business Continuity Plans based on clearly defined roles?
Yes

2.17.0.2.8 A process in place to ensure all employees are aware of their responsibilities and contact points in a continuity situation?
Yes

2.17.0.2.9 A requirement to review this policy annually?
Yes

2.17.0.2.10 A requirement for the relevant business to maintain Business Continuity Plans with defined recovery strategies to meet their recovery objectives on timescales and capacity?
Yes

2.17.0.2.11 Business Impact Analysis (BIAs) performed and reviewed at least annually, to understand the criticality, business impact, and required recovery times of your business processes?
Yes

2.17.1 Do you currently have a documented Business Continuity Plan?
Yes

2.17.1.25 Please give the date of the last review of your Business Continuity Plan.
14 07 2025

2.17.1.2 Does your company's Business Continuity Plan include the following:

2.17.1.3 Business Impact Assessments (BIA) for the products or services you will provide?
Yes

2.17.1.26 Integration of the current and potential impacts of climate change on your business?
Yes

2.17.1.28 Arrangements for loss of key dependencies (people, property, technology, data and supply chain) required for delivery of the products or services?
Yes - Data
Yes - People
Yes - Property
Yes - Supply Chain
Yes - Technology

2.17.1.29 The requirement to test Business Continuity Plans (through either desktop or live exercises) at least annually?
Yes

2.17.1.30 Test results formally documented and approved, including updating Business Continuity Plans for any issues identified during tests?
Yes

2.17.1.10 Is your Business Continuity Plan approved by senior management?
Yes

2.17.1.23 Does your company test your Business Continuity Plan?

Yes

2.17.1.22 Please give the date of your last successful test of your Business Continuity Plan.
31 10 2025

2.17.1.31 Does your company address any required improvements that are highlighted by tests of your Business Continuity Plan?
Yes

2.17.1.27 Does your Business Continuity Plan testing include:

2.17.1.27.1 Call cascading?
Yes

2.17.1.27.2 Discussion based exercises?
Yes

2.17.1.27.3 Scenario based exercises?
Yes

2.17.1.27.4 Workplace recovery testing?
Yes

2.17.1.27.5 Simulation testing?
Yes

2.17.1.27.6 Live testing?
Yes

2.17.18 Does your company regularly scan for threats against your organisation, either direct or indirect?
Yes

2.17.21 Does your company normally operate within defined impact tolerances for critical or important business services?
Yes

2.17.4 Does your company normally operate to planned Maximum Tolerable Period of Disruption (MTPD) for its business operations?
Yes

2.17.4.1 Does your company have geographically-separated primary and secondary data centres with identical infrastructure, hardware and software environments?
Yes

2.17.4.1.1 How many miles are there between your primary and secondary data centres?
10

2.17.4.5 Does your company complete regular Disaster Recovery Tests?
Yes

2.17.4.5.2 Are these Disaster Recovery Tests carried out in live production?
Yes

2.17.4.3 Please give the date of your last successful Disaster Recovery Test.
31 10 2025

2.17.4.5.3 If your disaster recovery test results in a failure, does your company retest it?
Yes

2.17.4.5.4 If your disaster recovery test results in a failure, within how many months is it

retested?
1

2.17.4.5.5 Does your disaster recovery testing provide assurance that services can operate from the secondary data centre across normal business processing days that include peaks of activity (e.g. full week)?
Yes

2.17.5 Please confirm that any critical suppliers or outsourcing providers have business continuity arrangements and testing in place to prevent disruption to the delivery of your products or services.
Yes

2.17.7 What is the Recovery Time Objective (RTO)?
2-4 hours

2.17.8 What is the Recovery Point Objective (RPO)?
>60 minutes

2.17.22 What is the Recovery Point Objective (RPO) based on Storage Area Network (SAN) mirroring/replication between data centres/availability zones?
>60 minutes

2.17.23 What is the Recovery Point Objective (RPO) based on restore from backups?
>60 minutes

2.17.9 Is the disaster recovery environment capable of running until the production environment is restored?
Yes

2.17.10 Does your disaster recovery environment provide the same capacity and performance of your production environment?
Yes

2.17.11 Does your company have overall resilience to achieve the Recovery Time Objective (RTO) of your business processes?
Yes

2.17.24 Has your business continuity or related testing confirmed that your company can achieve the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) of your business processes within the maximum tolerable duration of a disruption?
Yes - RPO
Yes - RTO

2.17.12 Does your company undertake incident root cause analysis and trend analysis?
Yes

2.17.13 Are controls in place to detect applications, systems or processes from reaching or exceeding capacity thresholds?
Yes

2.17.14 Do you currently have a documented IT Disaster Recovery Plan?
Yes

2.17.17 Are your IT services resilient against the loss of application(s) or infrastructure layer?
Yes

2.17.19 Does accountability for your company's operational resilience rest with your board and/or senior management?
Yes

2.17.20 Does your company have documented Crisis and Incident Management plans?
Yes

2.17.20.2 Please give the date of the last review of your Crisis and Incident Management plans.
10 09 2025

2.17.20.3 Does your company test your Crisis and Incident Management plans?
Yes

2.17.20.3.1 Please give the date of the last successful test of your Crisis and Incident Management plans.
31 10 2025

2.17.25 Do your Crisis and Incident Management plans include the following:

2.17.25.1 A requirement to test incident response capabilities at least annually and update any arrangements where appropriate?
Yes

2.17.26 Has your company sustained a major business outage in the last 12 months that impacted your clients?
No

2.18 Information Security

2.18.1 Does your company have a documented Information Security policy?
Yes – Willing to Upload Document

2.18.1.1 Please upload your Information Security policy.
Information Security Policy.pdf

2.18.1.2 Is your Information Security policy reviewed at least annually?
Yes

2.18.20 Does your information Security Policy contain the following elements:

2.18.20.1 Controls for testing and applying security patches?
Yes

2.18.20.2 Controls for secure system development & testing?
Yes

2.18.20.4 Password policy enforcing strong passwords?
Yes

2.18.20.5 A clear desk policy?
Yes

2.18.20.6 Disposal of all your clients information in a secure manner?
Yes

2.18.20.7 Exit strategy for the termination or Decommissioning of information and/or infrastructure at the end of the contract?
Yes

2.18.20.8 Key systems including applications set to log key events at all times?
Yes

2.18.20.9 The review of key system logs by an independent function on a regular basis to detect for any unauthorised activities?
Yes

2.18.20.10 Audit reviews and monitoring of resulting actions?
Yes

2.18.20.11 Information, software and system images are backed up and tested?
Yes

2.18.20.12 Baseline security documentation for ensuring Internet of Things (IoT) devices and associated services are protected?
Yes

2.18.20.13 Storage or transfer of client's data on any form of Internet of Things (IoT) device?
Yes

2.18.20.15 Addressing relevant information security risks arising from remote working?
Yes

2.18.38 Does your company have an annual information security improvement plan?
Yes

2.18.39 Does your company have a dedicated information security function or department?
Yes

2.18.17 Do you currently have an in-house documented Information Security management system?
Yes

2.18.25.12 Does your company have backup policies and procedures in place?
Yes

2.18.25.7 Does your company deploy backup mechanisms?
Yes

2.18.25.8.1 Please select which backup mechanisms your company deploys.
Differential Backups
Full Backups
Incremental Backups

2.18.25.8.2 Does your company test the restoration of the backups?
Yes

2.18.25.8.3 How many miles between your data centre and where your backups are stored?
280

2.18.25.8.4 How many months are there between tests of your backup and restoration procedures?
1

2.18.25.8.5 Are the results of the backup and restoration tests checked against production systems to ensure the integrity of the data and that records are complete?
Yes

2.18.25.8.6 Does your company take immutable backups?
Yes

2.18.25.8.7 Does your company implement the 3-2-1 backup strategy?
Yes

2.18.25.9 Does your company use a data vault to enable recovery from a ransomware attack or similar?
Yes

2.18.49 Does your company conduct internal vulnerability scans at least monthly?
Yes

2.18.50 Does your company conduct external vulnerability scans at least monthly?
Yes

2.18.37 Does your organisation have a documented process specifying remediation timelines for vulnerabilities?
Yes – Willing to Upload Document

2.18.37.1 Please select which categories of vulnerability your company's process covers.
Critical
High
Low
Medium

2.18.37.2 Please upload your company's process for specifying remediation timelines.
Patch Management Procedure.pdf

2.19 Cyber Security

2.19.1 Does your company have a documented cyber security response plan?
Yes

2.19.1.1 Is your company willing to provide a copy of your cyber security response plan so that your clients may evidence your management of cyber threats?
Yes

2.19.2 Does your cyber security response plan include the following:

2.19.2.1 Accountabilities and responsibilities based on clearly defined roles?
Yes

2.19.2.2 An identified source of cyber threat intelligence to continually improve your process?
Yes

2.19.2.3 Regular management information reports?
Yes

2.19.2.4 Processes and technologies to identify and treat cyber security incidents?
Yes

2.19.3 Does your company conduct cyber attack simulations to test your company's readiness to react to cyber threats and incidents?
Yes

2.19.3.3 Please give the date of the last cyber attack simulation.
31 10 2025

2.19.3.2 Does your company commission Red Team testing to help identify cyber security vulnerabilities?
No

2.19.4 Do you conduct Social Engineering testing on colleagues?
Yes

2.19.5 Does your company monitor the locations of devices connecting remotely?
Yes

2.19.6 Does your company provide specific training that covers remote/home working?
Yes

2.19.25 Is Mobile Device Management (MDM) implemented for remote workers, with VPN and/or Multi-Factor Authentication (MFA) in place?
Yes

2.19.7 Does your company disable by default the connection to personal/local printers?
Yes

2.19.8 Does your company have a documented Asset Management policy?
Yes

2.19.9 Does your company have a process for the disposal and/or destruction of physical media?
Yes

2.19.10 Does your company conduct internal and/or external audit and assurance processes in relation to Cyber Security?
Yes

2.19.11 Is your company willing to provide the appropriate documentation, upon request, so that your clients may evidence your audit and assurance processes in relation to Cyber Security?
Yes

2.19.12 Are remediation plans in place to implement any corrective action upon audit findings?
Yes

2.19.13 Does your company have a documented Cryptography, Encryption and Key management policy?
Yes

2.19.14 Does your company have a Cyber Security Governance process?
Yes

2.19.14.1 Do you review your Cyber Security Governance process at least annually?
Yes

2.19.14.2 Please confirm the date of the last review.
19 05 2026

2.19.15 Does your company have procedures in place for the tracking and logging of any hardware device containing your client's data which has been taken off-site?
Yes

2.19.16 Does your company conduct any software engineering activities, or include any software or firmware in any of your products?
Yes

2.19.17 Does your company have a documented Systems Development Life Cycle (SDLC) process for application design, development, deployment and operation capabilities?
Yes

2.19.18 Do systems and network devices used by your organisation utilise a common time synchronisation service?
Yes

2.19.19 Does your company operate a 24 hour Security Operations Centre (SOC)?
No

2.19.20 Does your company have Security Information and Event Management (SIEM) technology to support threat detection?
Yes

2.19.22.1 Please upload your Cyber Essentials Certificate.
Recite Me - Cyber Essentials (April 2026-2027).pdf

2.19.22.2 Please enter your Cyber Essentials Certificate expiry date.
14 04 2027

2.19.23.1 Please upload your Cyber Essentials Plus Certificate.
Recite Me - Cyber Essentials Plus (April 2026-2027).pdf

2.19.23.2 Please enter your Cyber Essentials Plus Certificate expiry date.
23 04 2027

2.19.24 Does your company use cyber intrusion detection and/or prevention systems (IDS/IPS) to monitor for cyber threats?
Yes - IDS and IPS

2.20 Technology

2.20.7 Does the data centre have any Wireless Access Points installed?
Yes

2.20.7.1 Are controls in place to detect and prevent unauthorised access?
Yes

2.20.8 Do all web applications your company uses to store or process your client's data have distributed denial-of-service (DDoS) protection?
Yes

2.20.8.1 Has DDoS mitigation protection been tested in the last year?
Yes

2.20.8.2 Do you test and protect against OWASP Top 10 vulnerabilities for web application services passing over public networks?
Yes

2.20.9 Is your company involved in any aspect of the design, development or testing of technology for your clients?
Yes - Design
Yes - Development
Yes - Testing

2.20.9.1 Does your company have segregated development, testing and production environments?
Yes

2.20.9.2 Are functional test environments up-to-date and reflective of the live environments?
Yes

2.20.9.3 Is open source software used in the provision of your company's services?
Yes

2.20.9.4 Do all IT changes have an approved recovery plan in place prior to the change being implemented?
Yes

2.20.10 Is your company responsible for the deployment of technology changes into the live production environment for your clients?
Yes

2.20.10.1 Is deployment done independently of the client or under supervision/approval?
Deployment is done independently of the client

2.20.11 Does your company have a documented currency or lifecycle management process for any hardware or software provided to your clients?
Yes - no review frequency specified in process

2.20.12 Is an asset inventory in place for all technology services provided to your clients?
Not required for the type of technology service provided

2.20.13 Does your company operate an automated technology batch type operation for any services provided to your clients?
No

2.20.14 Does your company have a documented capacity management process in place for any technology service provided to your clients?
Yes

2.20.14.1 Does your documented capacity management process include any of the following:
Alert Monitoring
Trend analysis of capacity usage

2.20.15 Does your company provide any network services, infrastructure or applications based on cloud computing?
Yes

2.20.15.1 Please select the type of cloud services you provide:
Hybrid Cloud

2.20.15.2 Please select the locations where your company stores any back-ups for your cloud services:
UK

2.20.15.3 Are any third parties used in the provision of your company's cloud services?
Yes

2.20.15.3.1 Please select the locations of any third parties used in the provision of your company's cloud services:
United Kingdom

2.20.15.3.2 Please select the name(s) of any third parties used in the provision of your company's cloud services.
Amazon Web Services (AWS)
CloudFlare
Google Cloud
Microsoft Azure
OVHcloud

2.20.15.3.4 Please select the type of cloud models used by these third parties for the provision of your

cloud services.
Private
Public

2.20.15.3.5 Please select the type of cloud services provided by these third parties for the provision of your cloud services.
Infrastructure as a Service (IaaS)

2.20.15.3.6 Please select the countries where data held by these third parties is backed up for the provision of your cloud services.
United Kingdom

2.20.15.3.7 Does your company have a process to gain a complete view of your third party's cloud security risks?
Yes

2.20.15.4 Has your organisation implemented the Shared Security Responsibility Model (SSRM) with any of your third-party providers and sub-contracting organisations?
Yes

2.20.15.4.1 Does your company review and update, where applicable, all SSRM documentation for the cloud services used at least annually?
Yes

2.20.15.5 Does your company have a documented cloud management policy in place?
Yes

2.20.16 What is the nature of client data held or processed in the cloud environment?
Confidential
Private
Public
Sensitive

2.20.19 Does your company maintain a Software Bill of Materials (SBOM) of all components in each of your software releases?
Yes

2.20.20 Does your company have a process in place to maintain a complete and accurate record of all application interfaces and application-to-application connections?
Yes - no material gaps or deficiencies in the process

2.21 Records Management

2.21.1 Does your company have a documented Records Management policy?
Yes – Not Willing to Upload Document

2.21.2 Does your Records Management policy and/or process include the following requirements:

2.21.2.2 A records inventory for all records created, received, stored, processed or destroyed on behalf of your clients?
Yes

2.21.2.3 Records retrieval procedures?
Yes

2.21.2.4 Records destruction procedures?
Yes

2.21.2.5 Legal Hold procedures?
Yes

2.21.2.6 Records handover procedures?
Yes

2.21.2.7 Records retention procedures?
Yes

2.21.2.8 Accountabilities and responsibilities based on clearly defined roles?
Yes

2.21.2.9 Identification and management of Records Management risks and incidents?
Yes

2.21.2.10 Records storage procedures?
Yes

2.21.2.11 Training on this process at least annually for all staff?
Yes

2.21.2.12 Protection of records against accidental or deliberate misuse, damage or destruction?
Yes

2.21.2.14 The ability to provide a recognised formal Certification of Destruction providing certified proof that data has been destroyed?
Yes

2.21.4 Does your company have a named person who is responsible for Records Management?
Yes

2.21.5 Please confirm trigger events and retention periods are in place in line with the third party policy summary for all client owned records managed by your company.
Yes

2.21.6 Does your company maintain a complete and detailed inventory of the legal and regulatory requirements for record-keeping?
Yes

2.21.7 Does your company have a data/record disposition arrangement set out?
Yes

2.22 Data Privacy

2.22.1 Does your company have a documented Data Privacy & Protection policy?
Yes – Not Willing to Upload Document

2.22.2 Does your Data Privacy & Protection policy and process include the following:

2.22.2.2 Definition of what personal data is collected?
Yes

2.22.2.3 Definition of when the individual's permission is sought?
Yes

2.22.2.4 Management of Data Subject Access Requests (DSAR)?
Yes

2.22.2.5 Protection of personal data against accidental or deliberate misuse, damage or destruction?

Yes

2.22.2.7 Handling complaints against any reported personal data issues?
Yes

2.22.2.8 Training on this process at least annually for staff who have data privacy responsibilities?
Yes

2.22.2.9 Regular assessments to identify where data privacy risks may not be sufficiently mitigated?
Yes - Both

2.22.2.10 Primary data privacy responsibilities for employee and subcontractors?
Yes

2.22.2.11 Alignment of data protection privacy principles to your companies obligations?
Yes

2.22.2.12 Confirmation that your company will only process data for specific purposes, and will not use it for any other incompatible purpose?
Yes

2.22.4 Are you registered as a data controller with the Information Commissioner's Office (ICO) in the United Kingdom?
Yes

2.22.4.1 Please provide your ICO Registration Number.
ZA485564

2.22.5 Is your company acting as a Data Controller, a Data Processor or a Joint Controller (with your clients)?
Data Processor

The following questions specifically relate to the specific requirements of the EU General Data Protection Regulation (GDPR) including the UK Data Protection Act 2018 and all types of personal data, including special categories of data. For more information please click [here|https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr]

2.22.29 Is your company compliant with the EU General Data Protection Regulation (GDPR), UK Data Protection Act 2018 and all other applicable privacy laws?
Yes

2.22.9 Does your company (or any subcontractors) transfer or process personal data outside of the UK or the EEA belonging to your clients?
Yes

2.22.9.1 Which of the following safeguards does your company use to ensure the transfer, processing or access to personal data outside of the UK or the EEA is compliant with the GDPR?
EU Adequate Countries
EU Standard Contractual Clauses
IDTA
IDTA Addendum
UK Adequate Countries
UK Standard Contractual Clauses

2.22.9.2 Has your company carried out a risk assessment on whether the right level of protection is in place in relation to the transfer, processing or accessing of personal data outside of the UK or the EEA?
Yes

2.22.9.3 Does your company have procedures to inform and obtain approval from your customers in case any personal or corporate data is to be processed by, or transferred to, any fourth party?
Yes - inform and obtain approval

2.22.10 Is your company compliant with all applicable data privacy legislation and/or regulation in all the jurisdictions in which your company operates?
Yes

2.22.12 Will your company (or any subcontractor) be processing special categories of personal data?
No

2.22.13 Does your company maintain an up-to-date and documented data diagram that shows how all personal data is received, stored, processed and transmitted (including by any subcontractors)?
Yes

2.22.39 Does your company have documented and approved procedures in place to regularly review and update the inventory of all personal data, including special categories of personal data, that you process, store or transfer to ensure that they are complete and traceable (including by any subcontractors)?
Not in place, work in progress but not committed to dates

2.22.15 Does your company have contracts in place with all subcontractors involved in the storage, processing and transmission of all personal data, which ensure your subcontractors are able to support your clients with data privacy and GDPR compliance?
Yes

2.22.43 Does your company (including any subcontractors) have the capability to erase all personal data belonging to your clients, upon request from your clients, without undue delay?
Yes – longer than 7 working days

2.22.18 Does your company (including any subcontractors) have the capability to provide all personal data to your clients that is being collected or processed on their behalf, upon their request?
Yes – within 2 working days

2.22.19 Does your company have documented and approved procedures in place to apply the principles of data protection by design and default (as defined in the GDPR)?
Yes, completed and currently in place

2.22.19.1 Do the procedures include any of the following safeguards into the design of processes and processing of personal data, including special categories of personal data?
Data minimisation
Encryption
Integration
Other Safeguards
Pseudonymisation

2.22.19.2 Are these safeguards applied to all data, not just personal data as defined by GDPR?
Yes

2.22.21 Does your company have documented and approved procedures to identify, document, remediate and notify your clients of any personal data breach without undue delay?
Yes - within 24 hours

2.22.22 Does your company have a designated Data Protection Officer or other named person

within the UK or EU who is responsible for Data Privacy or Protection?
Yes, completed and currently in place

2.22.23 Does your company have documented and approved plans in place to ensure that staff, contractors, consultants and subcontractors are trained at least annually and made aware of their roles and responsibilities in relation to UK GDPR, UK Data Protection Act 2018 and all other applicable privacy laws?
Yes, completed and currently in place

2.22.23.1 Does your company maintain records of such training?
Yes, completed and currently in place

2.22.23.2 Does your company ensure that staff, contractors, consultants and subcontractors sign a confidentiality agreement?
Yes, completed and currently in place

2.22.24 Does your company have a documented, implemented and client approved data retention schedule in place which covers your client's personal data, including special categories of personal data?
Yes, completed and currently in place

2.22.25 Does your company have a documented, implemented and client approved process to rectify or change your client's personal data including special categories of personal data, upon request?
Yes, completed and currently in place

2.22.26 Does your company complete privacy assessments for high risk activities?
Yes, completed and currently in place

2.22.27 Please select all countries where your company processes personal data including special categories of personal data.
Australia
United Kingdom
United States of America

2.22.30 What type of data are you collecting and/or processing on your clients behalf?
Client's customer data
Client's employee data

2.22.31 Do you or any of your subcontractors perform Automated Decision Making on behalf of your clients which have a legal or similarly significant effect on individuals?
No

2.22.32 Does your company have a documented process in place for you or your client to supply individuals with a Privacy Notice, in line with GDPR Requirements?
Yes

2.22.33 Does your company have a documented process to manage, record and evidence individuals' consent in relation to special categories of data?
Yes

2.22.33.1 Does your company have a documented process for the withdrawal of consent?
Yes

2.22.34 Does your company encrypt data at rest and/or in transit?
At Rest and In Transit

2.22.35 Does your company have a documented metadata management framework in place?
No

2.22.37 Does your company have a documented framework in place for effectively managing data quality throughout its lifecycle?
No

2.22.40 Does your company have procedures to manage your legal, regulatory and contractual obligations around data privacy?
Yes

2.22.41 Does your company have data governance processes in place to prevent incidents or failures arising from an insufficient understanding of the types of data being processed, data ownership, data quality, and the location of data at rest?
Yes

2.22.42 Does your company have trusted/golden sources and data lineage processes in place?
Yes

2.23 Supply Chain

2.23.11 Are any of your company's suppliers or subcontractors critical to the supply of goods or services provided to your clients in the financial services industry?
No

2.23.22 Does your company have a written policy and/or documented processes for managing sourcing and supply chain risk?
Yes – Willing to Upload Document

2.23.22.1 Please upload your policy and/or documented processes for managing sourcing and supply chain risk.
Supplier and Third-Party Management Policy.pdf

2.23.4.2 Does your Sourcing and Supply Chain Risk policy or documented processes include:

2.23.4.3 Identification and understanding of any risks and/or issues with the suppliers of your key services, prior to signing a contract/agreement?
Yes

2.23.4.4 Mitigation of any risk and/or issues identified as part of the supplier assessment?
Yes

2.23.4.5 Ongoing due diligence to ensure the risk assessment is up to date?
Yes

2.23.4.6 Structured ongoing supplier management to ensure supplier performance supports your key business processes?
Yes

2.23.4.7 Identification of key subcontractors that support key business processes?
Yes

2.23.4.8 Monitoring of the financial stability of your suppliers/subcontractors?
Yes

2.23.5 Does your company have documented controls in place to ensure suppliers/ subcontractors are performing as required under any contract and SLA agreed with your

clients?
Yes

2.23.6 Does your company confirm that those suppliers/subcontractors named above comply with your own policies?
Yes

2.23.8 Do your third party contracts contain anti-bribery provisions?
Yes

2.23.10 Does your company complete a supply chain risk analysis?
Yes

2.23.21 Do your company's third party contracts include clauses that support your client's rights to audit their processes?
Yes

2.23.23 Does your company have a Supplier Code of Conduct that your suppliers/subcontractors are required to comply with?
No

2.23.24 Does your company have a documented process and/or procedure in place with your suppliers/subcontractors for the identification, notification, reporting and resolution of any data breach within an agreed timeframe?
Yes

2.23.25 Does your company have documented and agreed incident management processes with your suppliers/subcontractors?
Yes

2.23.26 Does your company assess the effectiveness of supplier/subcontractor Business Continuity and IT Disaster Recovery plans?
Yes

2.23.27 Does your company have up-to-date exit plans (in both stressed and non-stressed scenarios) for suppliers/subcontractors that support the service provided to your clients?
Yes - Non-stressed
Yes - Stressed

2.23.28 Does your company maintain a list/database of all suppliers/subcontractors you rely on to provide services to your clients?
Yes

2.24 Diversity & Inclusion

2.24.1 Does your company have a documented Diversity & Inclusion policy?
Yes – Willing to Upload Document

2.24.1.1 Please upload a copy of your Diversity & Inclusion policy.
Diversity and Inclusion policy - Jan 25 (2).pdf

2.24.1.2 Please give the date of the last review of your Diversity & Inclusion policy.
14 01 2025

2.24.2 Does your documented Diversity & Inclusion policy include the following:

2.24.2.3 A named senior manager, director or board member responsible for Diversity & Inclusion?
No

2.24.2.6 Active encouragement of under-represented groups to apply for job vacancies?
Yes

2.24.2.7 Commitment in providing a work environment free from discrimination and harassment on any grounds protected by the UK Equality Act 2010 and any equivalent legislation or regulation in other jurisdictions in which your company operates?
Yes

2.24.2.8 Identifying incidents of bullying or harassment based on sexual orientation, gender identity, race, ethnicity, or disability?
No

2.24.2.9 Controls to prevent discrimination, bullying or harassment based on sexual orientation, gender identity, race, ethnicity, or disability?
No

2.24.4 Are your company's products or services accessible to customers with disabilities including visual or hearing impairment?
Yes

2.24.5 Are your company's IT systems and websites used by employees, customers or suppliers accessible to all users including people with disabilities?
Yes

2.24.11 Is your company a member or signatory of any of the following bodies:
No

2.24.12 Does your company measure how you are performing on Diversity & Inclusion?
No

2.24.13.0 Does your company have a supplier diversity programme in place?
No

2.24.14 Is your company majority owned by a representative of a minority group?
No

2.24.15 Does your company officially support any charity, community or volunteering initiatives?
No

2.24.16 Does your company measure the percentage of people from underrepresented groups in senior management positions?
No

2.24.17 Are your company's products and services compliant with the European Accessibility Act?
Yes

2.24.18 Does your company actively engage social enterprises as part of its supply chain strategy or sourcing practices?
No

2.25 Labour Standards

2.25.1 Does your company have a written policy and/or documented processes relating to Labour Standards?

No

2.25.2.0 Has your company carried out risk assessments to identify any Modern Slavery risks in your operation or supply chain?
Yes

2.25.2 Has your company identified any Modern Slavery risks in your operation or supply chain?
No risks identified

2.25.4 Has your company had any employment tribunal claims brought against it in the past 3 years?
No

2.25.19 Does your company provide staff with training on modern slavery?
Yes

2.25.8 Do you carry out internal audits and internal checks to ensure that modern slavery or related practices are not occurring within your organisation?
Yes

2.25.8.1 Have any modern slavery or related practices ever been identified within your organisation as a result of these audits?
No practices identified

2.25.10 Do you have terms and conditions with your suppliers which specifically forbid the use of slavery, servitude and forced or compulsory labour; and human trafficking?
No

2.25.11 Do you require that your suppliers carry out training to raise awareness of such practices in your supply chain and to ensure transparency and cooperation to resolve issues?
No

2.25.12.0 Does your company carry out supplier audits and checks to ensure that modern slavery or related practices are not occurring in your supply chain?
Yes

2.25.12.1 How frequently do these audits take place?
Annually

2.25.12.2 Does your company maintain records of these audits?
Yes

2.25.12.3 Have any modern slavery or related practices ever been identified within your supply chain as a result of these audits?
No practices identified

2.25.13 Does your company ensure all workers are paid at least the official national minimum wage?
Yes

2.25.14 Do you employ staff in any of the following categories:

2.25.14.1 Low skilled workforce
No

2.25.14.2 Seasonal / Temporary Staff
No

2.25.14.3 Migrant Workers

No

2.25.14.4 Do any of your company's employees operate on zero hour contracts?
No

1.7.6.8 Has your company previously been investigated or convicted by a competent authority (e.g. a Government organisation or a multilateral body such as the United Nations) for any activities relating to slavery, servitude, child, forced and compulsory labour and human trafficking?
No

2.25.20 Does your company have documented policies or procedures relating to the prevention of sexual harassment?
Yes

2.25.21 Do your company's policies or processes relating to the prevention of sexual harassment include the following:

2.25.21.1 Commitment to providing a work environment free from sexual harassment?
Yes

2.25.21.2 Procedures for identifying, addressing, and reporting incidents of sexual harassment?
Yes

2.25.21.3 Regular training for employees and workers on preventing sexual harassment?
Yes

2.25.21.4 Measures to protect employees and workers from victimisation for reporting sexual harassment?
Yes

2.26 Environment

2.26.1 Does your company have an Environmental Policy?
Yes – Willing to Upload Document

2.26.2 Please upload a copy of your Environmental Policy.
Environmental-policy - Jan 24.pdf

2.26.6 Has your company been served with a prosecution/enforcement notice by the Environment Agency or equivalent body outside the UK in the past 5 years?
No

2.26.24 Do your company's environmental policies or documented procedures include, or reference, your approach to the following:

2.26.24.1 Pollution?
No

2.26.24.2 Biodiversity and ecosystems?
No

2.26.24.3 Water and marine resources?
No

2.26.24.4 Energy use?
No

2.26.24.5 Waste?
No

2.26.5 Do you currently have an in-house documented environmental management system which your client is able to inspect upon demand?
No

2.26.15 Does your company have any documented practices in place to reduce waste to landfill?
Yes

2.26.25 Does your company use Single Use Plastics (SUP)?
No

2.26.36 Does your company supply any physical goods as part of the services you provide to clients?
No

2.26.8 Does your company have a documented process for assessing the impacts that climate change will have on your company?
No

2.26.8.1 Does your company have plans to implement a process for assessing the impacts that climate change will have on your company?
No

2.26.9 Does your company have a process for assessing the impacts that climate change will have on your supply chain?
No

2.26.10 Does your company have a process for assessing the opportunities climate change may present to your company?
No

2.26.16 Does your company have a Sustainable Procurement policy?
No

2.26.26 Does your company have plans in place to reduce your environmental impact in any of the following areas?
No

2.26.37 Does your company measure greenhouse gas emissions?
No

2.26.14 What percentage of your company's electricity usage in the latest reporting period was from renewable sources?
25

2.26.34 Is your company a member or signatory of any of the following ESG bodies or ratings agencies:
No

2.26.39 Does your company complete the CDP Climate Change questionnaire on an annual basis?
No

2.32 Financial & Legal

2.32.1 If the financial accounts fields are not pre-populated by Company Watch please click 'Add new Company Accounts' to provide company accounts for each of the past three years. Please enter the full figures in GBP or EUR for the exact company/legal entity being registered. If accounts are held in another currency please convert into GBP or EUR using the prevailing exchange rate. If you need to add a new Financial Year, please click 'Add new Company Accounts'.

2.32.1.1 Financial Year
2025

2.32.1.1.1 Currency
GBP

2.32.1.2 Revenue
6005082

2.32.1.3 Pre-tax Profit/Loss
-1040603

2.32.1.4 Cash & Cash Equivalents
1198778

2.32.1.5 Other Debtors Etc
422142

2.32.1.6 Fixed Assets
3071505

2.32.1.7 Current Assets
2381870

2.32.1.8 Current Liabilities
4653967

2.32.1.9 Long-term Liabilities
1116655

2.32.1.10 Shareholders' Funds
-317247

2.32.1.1 Financial Year
2024

2.32.1.1.1 Currency
GBP

2.32.1.2 Revenue
4740679

2.32.1.3 Pre-tax Profit/Loss
-1064646

2.32.1.4 Cash & Cash Equivalents
820473

2.32.1.5 Other Debtors Etc
348627

2.32.1.6 Fixed Assets
2325423

2.32.1.7 Current Assets
1844393

2.32.1.8 Current Liabilities
3776343

2.32.1.9 Long-term Liabilities
974637

2.32.1.10 Shareholders' Funds
-581164

2.32.1.1 Financial Year
2023

2.32.1.1.1 Currency
GBP

2.32.1.2 Revenue
3445036

2.32.1.3 Pre-tax Profit/Loss
-1033501

2.32.1.4 Cash & Cash Equivalents
1557618

2.32.1.5 Other Debtors Etc
286425

2.32.1.6 Fixed Assets
1519235

2.32.1.7 Current Assets
2212030

2.32.1.8 Current Liabilities
2825657

2.32.1.9 Long-term Liabilities
740930

2.32.1.10 Shareholders' Funds
164678

2.32.2 Has your company had any County Court Judgements (CCJs) issued against it? *(optional)*
No

2.32.4 Is your company's beneficial owner a public official, or closely related to a public official?
No

2.32.5 Does your company have measures in place to ensure that 95% of small business invoices are paid within 30 days?
Yes

2.32.7 Has your Company signed up to a timely payment code in any jurisdiction in which it operates, for example in the UK, the Prompt Payment Code?
No

2.32.8 Has your company been suspended from any timely payment scheme in any jurisdiction in which it operates in the last 5 years?
No

2.32.9 Does your company ensure that a minimum living wage is paid in the jurisdictions in which it operates? For example, the Real Living Wage Foundation in the UK or Living Wage Technical Group in Ireland.
Yes - UK/Ireland

2.32.11 Does your company pay any workers off-payroll, such as through personal service companies or other intermediaries?
No

2.32.12 Does any individual working for you under contract own more than 5% of shares in your company or another company within your supply chain, or is any worker a member of a partnership in your supply chain?
Yes

2.32.13 Who performs the statutory audit of your company's financial statements?
Other

2.33 Insurances

2.33.1 Please provide details of your Employer's Liability insurance:

2.33.1.1 Level of cover
15000000

2.33.1.2 Currency of cover
GBP

2.33.1.3 Is this limit in aggregate or per claim?
Per Claim

2.33.1.4 Policy expiry date
13 03 2027

2.33.1.5 Please upload your insurance certificate or other evidence issued by your insurer, such as the insurance schedule.
2026 TWIMC UK .pdf

2.33.2 Please provide details of your Public Liability insurance:

2.33.2.1 Level of cover
10000000

2.33.2.2 Currency of cover
GBP

2.33.2.3 Is this limit in aggregate or per claim?
Per Claim

2.33.2.4 Policy expiry date
13 03 2027

2.33.2.5 Please upload your insurance certificate or other evidence issued by your insurer, such as the insurance schedule.
2026 TWIMC UK .pdf

2.33.3 Please provide details of your Professional Indemnity insurance:

2.33.3.1 Level of cover
10000000

2.33.3.2 Currency of cover
GBP

2.33.3.3 Is this limit in aggregate or per claim?
Per Claim

2.33.3.4 Policy expiry date
13 03 2027

2.33.3.5 Please upload your insurance certificate or other evidence issued by your insurer, such as the insurance schedule.
2026 TWIMC UK .pdf

2.33.6 Please provide details of your Cyber Liability insurance:

2.33.6.1 Level of cover
2000000

2.33.6.2 Currency of cover
GBP

2.33.6.3 Is this limit in aggregate or per claim?
Per Claim

2.33.6.4 Policy expiry date
13 03 2027

2.33.6.5 Please upload your insurance certificate or other evidence issued by your insurer, such as the insurance schedule.
2026 TWIMC UK .pdf

2.33.7 Please provide details of your Products Liability insurance:

2.33.7.1 Level of cover
5000000

2.33.7.2 Currency of cover
GBP

2.33.7.3 Is this limit in aggregate or per claim?
Per Claim

2.33.7.4 Policy expiry date
13 03 2027

2.33.7.5 Please upload your insurance certificate or other evidence issued by your insurer, such as the insurance schedule.
2026 TWIMC UK.pdf

2.37 Artificial Intelligence

2.37.1 Does your company (including any subcontractor) use Artificial Intelligence (AI) at any stage in the delivery of your products or services?
Yes

2.37.1.1 Please select which specific AI technologies and tools are being used in the delivery of your products or services.
Generative AI

2.37.2 Does your company have an Artificial Intelligence (AI) policy?
Yes – Not Willing to Upload Document

2.37.3 Does your Artificial Intelligence policy include the following:

2.37.3.1 The requirement to assess and mitigate the risks associated with your use of AI?
Yes

2.37.4 Has your company implemented an AI framework to ensure responsible and ethical use of AI?
Yes

2.37.5 Is your company using AI to support any of the following types of activity?
No

2.37.6 Does your company use customer data to train/develop your AI model?
No

2.37.7 Does your company have controls in place to prevent data poisoning attacks in the AI models you use?
Yes

2.37.8 Does your company or any subcontractor process personal information shared by your customers in an AI system?
Yes

2.37.9 Does your company or any subcontractor process sensitive personal information shared by your customers in an AI system?
No

2.37.10 Can customers opt-out of such personal information use?
Yes

2.37.11 How is personal or sensitive data protected and anonymised in AI processes?
Access Controls
Data Encryption
Data Masking
Data Minimisation
Pseudonymisation
Regular Audits and Compliance Checks

2.37.12 Does the AI system create new information that can be associated with an individual?
No

2.37.17 Does your company have documented processes in place to test the AI system for biases and other unexpected outcomes?
Yes

2.37.18 Is the AI system monitored for accuracy, with an option for human override?
Yes

2.37.19 Has your company received any privacy complaints from individuals related to the use of AI systems?
No

2.37.20 Does your company have controls in place to regularly assess the performance of the AI systems you use and incorporate feedback for continuous improvement?
Yes

2.37.21 Does your company have controls in place to prevent copyright infringement when using AI?
Yes

2.37.22 Does your company have controls in place to identify and stop/reduce the use of shadow AI within your organisation?

Yes

2.37.23 Does your company have an incident response plan specifically for AI-related incidents?
Yes

2.38 Products & Services

2.38.1.1 Please complete the following questions for this product or service:
0523 - Software Development - Corporate

2.38.1.2 Description of the product or service supplied.
Accessibility software for use by our customers on their site(s) and / or application(s). This could include software to support accessibility on an application in a corporate environment or scan an internal application for accessibility issues.

2.38.1.3 Would your company like to upload a one page summary or brochure detailing this product or service?
No

2.38.1.1 Please complete the following questions for this product or service:
0525 - Software Development - Enterprise

2.38.1.2 Description of the product or service supplied.
Accessibility software for use by our customers on their site(s) and / or application(s). This could include software to support accessibility on an application in an enterprise environment or scan an internal application for accessibility issues.

2.38.1.3 Would your company like to upload a one page summary or brochure detailing this product or service?
No

2.38.1.1 Please complete the following questions for this product or service:
0537 - Software Development - Digital

2.38.1.2 Description of the product or service supplied.
Accessibility software for use by our customers on their site(s) and / or application(s). Our applications include a Toolbar which provides accessibility functions to end users of such sites / applications.

2.38.1.3 Would your company like to upload a one page summary or brochure detailing this product or service?
No

2.38.1.1 Please complete the following questions for this product or service:
0554 - Software Consultancy

2.38.1.2 Description of the product or service supplied.
Manual Web Accessibility Testing to WCAG 2.2

2.38.1.3 Would your company like to upload a one page summary or brochure detailing this product or service?
No

2.38.2 Does your company (or any of your subcontractors) use quantitative methods at any stage in the delivery of your product/service to your client?

No