

**Illustrative Questionnaire for the   
Due Diligence of   
Vendor Technology and Cyber Security**

|  |  |
| --- | --- |
| NAME OF COMPANY RESPONDING: | |
| Click here to enter text. | |
|  | |
| AS OF DATE OF THIS DDQ: | |
| Click here to enter a date. | |
|  | |
| CONTACT DETAILS FOR PERSON AT VENDOR TO DISCUSS THIS DDQ WITH: | |
| Click here to enter text. | |
|  | |
|  | Tick here if the vendor undertakes to notify the recipient of material changes that take place to answers provided in this DDQ |
| NAME OF REQUESTING AITEC/AIMA MEMBER: | |
| Click here to enter text. | |

PURPOSE

AITEC consists of over 400 CTO’s, CISO’s and other executive level technologists who work in the alternate investment space and AIMA has more than 1,800 members globally. AITEC and AIMA are currently looking to take advantage of their memberships’ scale by asking members to engage their vendor partners to participate in the DDQ program.

Essentially the program puts the vendor in control by leaving who gets access to their completed questionnaires up to them. Only AITEC and AIMA members who are your clients or prospects and who have executed their own confidentiality agreement with your firm will have access to your completed questionnaire.

**Members are forbidden from distributing your completed questionnaires to other members without explicit permission from your firm.**

Participation in the program simply requires that your firm have a completed copy on hand for members to request their own copies. It will be up to your firm and clients to negotiate a confidentiality agreement prior to sharing with them your completed questionnaire.

DISCLAIMER

None of AITEC, AIMA, or their respective officers, employees or agents makes any representation or warranty, express or implied, as to the adequacy, completeness or correctness of the questionnaire. No liability whatsoever is accepted by AITEC, AIMA, or their respective officers, employees or agents for any loss howsoever arising from any use of this questionnaire or its contents or otherwise arising in connection therewith. For the avoidance of doubt, note that, by providing this questionnaire, neither AITEC nor AIMA acts as legal counsel in any jurisdiction.

USE OF THIS QUESTIONNAIRE IS RESTRICTED

Members of AITEC and AIMA have a limited license to use this questionnaire while they are members in the circumstances set out in the Terms of Use. Vendors who are not members of AITEC or AIMA also have a limited license to use this questionnaire in the relevant circumstances set out in the Terms of Use. This license does not include permission to circulate this questionnaire to any other persons nor does it include permission for use by non-members in any other circumstances. The copyright in this questionnaire is the sole property of AITEC and AIMA. You may not distribute it or copy it for any purpose other than in line with the limited license set out above without prior written consent from AITEC and AIMA.

VENDOR CERTIFICATION

Vendors filling in this DDQ must make one of the certifications below. When the DDQ is provided in other than electronic platform format, the certification must appear in a location that is between the front cover page and the table of contents regardless of format.

|  |  |
| --- | --- |
| Tick the one that applies. If none do, then neither you nor your firm is authorised to distribute this DDQ under AITEC’s or AIMA’s copyright. | |
|  | I am a member of AITEC and I represent the vendor and *neither I nor the vendor have changed any of the questions or set response choices*. We have abided by the Terms of Use. |
|  | I am a member of AITEC and I represent the vendor and *some of the questions or set response choices have been changed and I have accordingly removed the AITEC and AIMA branding as required*. We have abided by the Terms of Use. |
|  | Our firm is a vendor that is a member of AIMA and *we have not changed any of the questions or set response choices*. We have abided by the Terms of Use. |
|  | Our firm is a vendor that is a member of AIMA and *we have changed some of the questions or set response choices and have accordingly removed the AITEC and AIMA branding as required*. We have abided by the Terms of Use. |
|  | Our firm is not itself a member of AIMA or represented by a member of AITEC but this DDQ was provided to our firm to fill in by a member of AIMA or AITEC. We understand that because our firm is not a member of AIMA or represented by a member of AITEC, our firm is not authorised under the copyright to supply a completed copy of this DDQ to anyone other than the providing member of AIMA or AITEC. *We have not changed any of the questions or set response choices*. We have abided by the Terms of Use. |
|  | Our firm is not itself a member of AIMA or represented by a member of AITEC but this DDQ was provided to our firm to fill in by a member of AIMA or AITEC. We understand that because our firm is not a member of AIMA or represented by a member of AITEC, our firm is not authorised under the copyright to supply a completed copy of this DDQ to anyone other than the providing member of AIMA or AITEC. *We have changed some of the questions or set response choices and have accordingly removed the AITEC and AIMA branding as required*. We have abided by the Terms of Use. |

[1. Company Information 1](#_Toc531184890)

[1.1 Contact Information 1](#_Toc531184891)

[1.2 Financial Matters 2](#_Toc531184892)

[1.3 Regulatory Matters 2](#_Toc531184893)

[1.4 Employment Screening 2](#_Toc531184894)

[1.5 Complaints and Litigation 4](#_Toc531184895)

[1.6 Additional Questions 4](#_Toc531184896)

[1.7 Company Comments 4](#_Toc531184897)

[2. Product/Service Information 4](#_Toc531184898)

[2.1 Relevant Product/Service 5](#_Toc531184899)

[2.2 Additional Questions 6](#_Toc531184900)

[2.3 Company Comments 6](#_Toc531184901)

[3. Policies, Procedures, Standards and Controls 7](#_Toc531184902)

[3.1 General 7](#_Toc531184903)

[3.2 Risk Management 8](#_Toc531184904)

[3.3 Change Management 9](#_Toc531184905)

[3.4 Identity and Access Management 9](#_Toc531184906)

[3.5 Awareness and Training 10](#_Toc531184907)

[3.6 Additional Questions 10](#_Toc531184908)

[3.7 Company Comments 10](#_Toc531184909)

[4. Data Security 11](#_Toc531184910)

[4.1 Data Management 11](#_Toc531184911)

[4.2 Encryption 11](#_Toc531184912)

[4.3 Mobile Access 12](#_Toc531184913)

[4.4 Data Loss Prevention 15](#_Toc531184914)

[4.5 Additional Questions 16](#_Toc531184915)

[4.6 Company Comments 16](#_Toc531184916)

[5. System Maintenance 16](#_Toc531184917)

[5.1 Asset Management 16](#_Toc531184918)

[5.2 Process 17](#_Toc531184919)

[5.3 Additional Questions 19](#_Toc531184920)

[5.4 Company Comments 19](#_Toc531184921)

[6. Access Controls 19](#_Toc531184922)

[6.1 Entitlements 19](#_Toc531184923)

[6.2 Client Access Controls 20](#_Toc531184924)

[6.3 Internal Staff Access Controls 22](#_Toc531184925)

[6.4 Additional Questions 23](#_Toc531184926)

[6.5 Company Comments 23](#_Toc531184927)

[7. Infrastructure Security 23](#_Toc531184928)

[7.1 Network Security 23](#_Toc531184929)

[7.2 Endpoint Security 25](#_Toc531184930)

[7.3 Penetration Testing 26](#_Toc531184931)

[7.4 Additional Questions 26](#_Toc531184932)

[7.5 Company Comments 26](#_Toc531184933)

[8. Physical Security 27](#_Toc531184934)

[8.1 Office Access Security 27](#_Toc531184935)

[8.2 Server Access Security 29](#_Toc531184936)

[8.3 Additional Questions 30](#_Toc531184937)

[8.4 Company Comments 30](#_Toc531184938)

[9. Business Continuity 30](#_Toc531184939)

[9.1 Policy 30](#_Toc531184940)

[9.2 Specifications 31](#_Toc531184941)

[9.3 Additional Questions 34](#_Toc531184942)

[9.4 Company Comments 34](#_Toc531184943)

[10. Cyber Incident Response 34](#_Toc531184944)

[10.1 Cyber Incident Response Plan 34](#_Toc531184945)

[10.2 Detection and Response 34](#_Toc531184946)

[10.3 Cyber Incidents 35](#_Toc531184947)

[10.4 Client Notification 35](#_Toc531184948)

[10.5 Cybersecurity Insurance 36](#_Toc531184949)

[10.6 Additional Questions 36](#_Toc531184950)

[10.7 Company Comments 36](#_Toc531184951)

[11. Software Development 37](#_Toc531184952)

[11.1 In-House Development Practices 37](#_Toc531184953)

[11.2 Outsourced Development Practices 38](#_Toc531184954)

[11.3 Additional Questions 38](#_Toc531184955)

[11.4 Company Comments 39](#_Toc531184956)

[12. Vendor Due Diligence by the Company 39](#_Toc531184957)

[12.1 Outsourcing 39](#_Toc531184958)

[12.2 Service Levels 39](#_Toc531184959)

[12.3 Additional Questions 40](#_Toc531184960)

[12.4 Company Comments 40](#_Toc531184961)

[13. Further Information: Critical Outsourced Functions 40](#_Toc531184962)

[13.1 Structure 40](#_Toc531184963)

[13.2 Further Regulatory and Financial Matters 41](#_Toc531184964)

[13.3 More Questions on Outsourcing by the Company to Third Parties 42](#_Toc531184965)

[13.4 Additional Questions 43](#_Toc531184966)

[13.5 Company Comments 43](#_Toc531184967)

[FURTHER INSTRUCTIONS 45](#_Toc531184968)

[TERMS OF USE 48](#_Toc531184969)

| 1. Company Information | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 4. | | | | | | | |
| 1.1 Contact Information | | | | | | | |
| 1.1.1  N/A More | What is the name of the vendor completing this DDQ (referred to in the DDQ as the ‘company’)? | | | | Click here to enter text. | | |
| 1.1.2  N/A More | Is the legal name of the company different from the name of the company completing this DDQ? | | | | Yes, and the company’s legal name is provided below.  No  Click here to enter text. | | |
| 1.1.3  N/A More | What is the company’s principal business address? | | | | Click here to enter text. | | |
| 1.1.4  N/A More | Is the registered address of the company different from its principal business address? | | | | Yes, and the company’s registered address is provided below.  No  Click here to enter text. | | |
| 1.1.5  N/A More | What is the company’s registration number? | | | | Click here to enter text.  Not applicable | | |
| 1.1.6  N/A More | What is the company’s website address? | | | | Click here to enter text. | | |
| 1.1.7  N/A More | (a) Does the company have a primary relationship manager? | | | | Yes  No, and, as a consequence, (b)-(e) below have been left blank.  No, and, as a consequence, the rows for Questions 1.1.7(b)-(e) in the template DDQ have been omitted. | | |
| N/A More | (b) What is the full name of the primary relationship manager? | | | | Click here to enter text. | | |
| N/A More | (c) What is the job title of the primary relationship manager? | | | | Click here to enter text. | | |
| N/A More | (d) What is the telephone number of the primary relationship manager? | | | | Click here to enter text. | | |
| N/A More | (e) What is the email address of the primary relationship manager? | | | | Click here to enter text. | | |
| 1.1.8  N/A More | Does the company have an information security contact that clients can reach out to directly? | | | | Yes, and contact details for that person are set out below.  No  Click here to enter text. | | |
| 1.2 Financial Matters | | | | | | | |
| 1.2.1  N/A More | Has the company ever received a qualified or going concern opinion with respect to its audited financial statements? | | | | Yes, and details are provided below.  No  Not applicable  Click here to enter text. | | |
| 1.2.2  N/A More | During the last five years (or the life of the company, if shorter), have all required tax returns been filed and taxes paid on time? | | | | Yes  No, and details are provided below.  Click here to enter text. | | |
| 1.3 Regulatory Matters | | | | | | | |
| 1.3.1  N/A More | Does the company require any authorization and/or registration with a regulatory authority in order to provide the relevant product and/or service? | | | | Yes, and the names(s) of the relevant regulator(s) together with the authorization and/or registration number(s) is provided below.  No  Click here to enter text. | | |
| 1.4 Employment Screening | | | | | | | |
| 1.4.1  N/A More | Which types of internal (i.e., performed by company personnel) and external (i.e., performed by a third-party vendor) background checks does the company conduct for each category of person/entity before they are hired and are granted access to sensitive data and how frequently are such checks made/renewed?  **Instructions:** For each type of check listed in the table below, indicate which types of persons are subject to that check and with what frequency (selecting as many of the frequency choices as apply in each case).  For companies employing more than 250 people, the response to this question may be limited to the C-suite and employees, consultants, external providers and others related to the relevant product and/or service. | | | | See table below.  The company has more than 250 employees and we have chosen to limit our response to this question in accordance with the instructions. See table below.  None, and, as a consequence, the table below has been left blank.  None, and, as a consequence, the rows containing the table following Question 1.4.1 in the template DDQ have been omitted. | | |
| Type of background  check | | Type of person/entity | | | | | |
| Permanent Employee | Temporary Employee | Consultant | | External Provider | Other |
| Credit (internal) | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable |
| Credit (external) | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable |
| Criminal (internal) | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable |
| Criminal (external) | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable |
| Drug (internal) | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable |
| Drug (external) | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable |
| Employment (internal) | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable |
| Employment (external) | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable |
| Other (internal) | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable |
| Other (external) | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable | Pre-hiring  On hiring  Annually  Ad hoc  Not applicable |
| 1.4.2  N/A More | Are employees, subcontractors and temporary workers with access to client data legally bound to confidentiality (whether separately or as part of their employment contract and/or code of conduct)? | | | | Yes  No | | |
| 1.4.3  N/A More | Are employees, subcontractors and temporary workers with access to client data, bound by the company’s Information Security Procedures? | | | | Yes  No | | |
| 1.4.4  N/A More | Does the company review/assess the security posture of all third parties that have access to the company’s client data or environment via their own systems? (*Select one*) | | | | Company personnel undertake this review/assessment with the assistance of an independent third-party firm.  Company personnel undertake this review/assessment without the assistance of any third parties.  An independent third-party firm performs this review/assessment for the company.  Not applicable | | |
| 1.5 Complaints and Litigation | | | | | | | |
| 1.5.1  N/A More | Have there been any prior lawsuits (in the last five years) to which the company was a party that involved allegations of privacy breaches or data breaches? | | | | Yes, and details are provided below.  No  Click here to enter text. | | |
| 1.5.2  N/A More | Are there any current or pending lawsuits to which the company is a party that involve allegations of privacy breaches or data breaches? | | | | Yes, and details are provided below.  No  Click here to enter text. | | |
| 1.5.3  N/A More | Are there any current or pending lawsuits that may reasonably affect the company’s ability to provide the relevant product and/or service if decided against the company? | | | | Yes, and details are provided below.  No  Click here to enter text. | | |
| 1.6 Additional Questions | | | | | | | |
| Further Question | Add a question below:  Click here to enter text. | | | | Click here to enter text. | | |
| 1.7 Company Comments | | | | | | | |
| Comment | Enter relevant question number:  Click here to enter text. | | | | Click here to enter text. | | |

| 2. Product/Service Information | | | | |
| --- | --- | --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 6. | | | | |
| 2.1 Relevant Product/Service | | | | |
| 2.1.1  N/A More | By what name does the company refer to the product and/or service to which the responses in the rest of the DDQ relate (the ‘relevant product and/or service’)? | Click here to enter text. | | |
| 2.1.2  N/A More | Please describe the nature of the relevant product and/or service. | Click here to enter text. | | |
| 2.1.3  N/A More | In what year did the company begin offering the relevant product and/or service? | Click here to enter text. | | |
| 2.1.4  N/A More | Please provide the number of employees providing the relevant product and/or service by location and department. | Location | Functional Area | Total Staff |
| Click here to enter text. | Product development  Product support  Product sales  Other | Click here to enter text. |
| Click here to enter text. | Product development  Product support  Product sales  Other | Click here to enter text. |
| Click here to enter text. | Product development  Product support  Product sales  Other | Click here to enter text. |
| 2.1.5  N/A More | To how many active clients does the company provide the relevant product and/or service? Please indicate whether this is the current peak. | Click here to enter text. | | |
| 2.1.6  N/A More | Does the company have any dedicated cyber security staff supporting the relevant product and/or service? | Yes  No | | |
| 2.1.7  N/A More | How many of the company’s active clients are in the business of hedge funds or alternative investment funds? | Click here to enter text. | | |
| 2.1.8  N/A More | (a) Does the company have a primary relationship manager for the relevant product and/or service who is different to the primary relationship manager for the company as a whole? | Yes  No, and, as a consequence, (b)-(e) below have been left blank.  No, and, as a consequence, the rows for Questions 2.1.8(b)-(e) in the template DDQ have been omitted. | | |
| N/A More | (b) What is the full name of the primary relationship manager in relation to the relevant product and/or service? | Click here to enter text. | | |
| N/A More | (c) What is the job title of the primary relationship manager in relation to the relevant product and/or service? | Click here to enter text. | | |
| N/A More | (d) What is the telephone number of the primary relationship manager in relation to the relevant product and/or service? | Click here to enter text. | | |
| N/A More | (e) What is the email address of the primary relationship manager in relation to the relevant product and/or service? | Click here to enter text. | | |
| 2.2 Additional Questions | | | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. | | |
| 2.3 Company Comments | | | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. | | |

| 3. Policies, Procedures, Standards and Controls | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 10. | | |
| 3.1 General | | |
| 3.1.1  N/A More | What aspects are covered in the company’s policies, procedures, standards and controls? *(Select all that apply)* | Acceptable use  Account/credentials management  Anti-virus and anti-malware  Clean desk  Data destruction  Email and messaging  Encryption  Multi-factor authentication  Network access  Passwords  Patch management  Personal/mobile devices  Personally-identifiable and/or sensitive information  Personnel security training  Physical security  Remote access  Removable media  Reporting security violations  Social media/networking  Software usage and licensing  Systems and software inventory  Systems monitoring  Third party/vendor access  Wireless network communications  Other (Provide additional comments)  Not applicable  Click here to enter text. |
| 3.1.2  N/A More | How often are the company’s written policies and procedures reviewed and updated? *(Select one)* | At least monthly  At least quarterly  At least semi-annually  At least annually  Other (Provide additional comments)  Not applicable  Click here to enter text. |
| 3.1.3  N/A More | Does the company make any exceptions to the security policy/processes for person or group of persons? *(Select all that apply)* | C-suite executives  Senior staff  Staff working remotely  Temporary employees  Consultants  Other (Provide additional comments)  No exceptions  Click here to enter text. |
| 3.1.4  N/A More | Does the company have any certifications or assessments relevant to information security? *(Select all that apply)* | ISO 27001  SSAE 16  ISAE 3402  PCI DSS  SOC 2  SOC 3  Other (Provide additional comments)  None (Provide additional comments)  Click here to enter text. |
| 3.2 Risk Management | | |
| 3.2.1  N/A More | Does the company manage risk specifically as it pertains to information security? | Yes  No, and, as a consequence, the rest of this section 3.2 has been left blank and an explanation is provided below.  No, and, as a consequence, the rows for Questions 3.2.2-3.2.4 in the template DDQ have been omitted and an explanation is provided below.  Click here to enter text. |
| 3.2.2  N/A More | What is covered in the company’s information security program? *(Select all that apply)* | Risk identification  Risk measurement  Risk mitigation  Risk monitoring  Risk reporting  Other (Provide additional comments)  None of the above  Click here to enter text. |
| 3.2.3  N/A More | How often are the information security risks reviewed and updated? *(Select one)* | At least monthly  At least quarterly  At least semi-annually  At least annually  Other (Provide additional comments)  Not applicable  Click here to enter text. |
| 3.2.4  N/A More | Does the company have a threat identification process to collect data on potential threats that is used to inform its information security risk assessment? | Yes, and details are provided below.  No  Click here to enter text. |
| 3.3 Change Management | | |
| 3.3.1  N/A More | Are policies or procedures in place to plan, manage, test, document and approve changes to production systems? | Yes, and a summary of the change management procedures is provided below.  No, and, as a consequence, an explanation has provided below, and Question 3.3.2 has been left blank.  No, and, as a consequence, an explanation has been provided below and the row for Question 3.3.2 in the template DDQ has been omitted.  Not applicable, and, as a consequence, an explanation has provided below, and Question 3.3.2 has been left blank.  Not applicable, and, as a consequence, an explanation has been provided below and the row for Questions 3.3.2 in the template DDQ has been omitted.  Click here to enter text. |
| 3.3.2  N/A More | Does the company have any special provisions in its change management policy to allow for emergency changes? | Yes, and details are provided below.  No  Not applicable  Click here to enter text. |
| 3.4 Identity and Access Management | | |
| 3.4.1  N/A More | Does the company have a standard identity and access management process governing the creation and management (including removal upon termination and adjustment on transfers) of network and application users that can access client data? | Yes  No |
| 3.4.2  N/A More | Do the company’s access control policies or procedures require that passwords are strong? *(Select all that apply)* | Requires at least 2 different character classes to be present in the password (uppercase, lowercase, special, number, etc.)  Requires at least 3 different character classes to be present in the password (uppercase, lowercase, special, number, etc.)  Length of 6 characters or more  Length of 8 characters or more  Length of 10 characters or more  Length of 12 characters or more  Disallows known weak passwords  Disallows previously used passwords  Other (Provide additional comments)  Click here to enter text. |
| 3.4.3  N/A More | Is the company’s access control policy configured to expire user passwords periodically? *(Select one)* | Yes, every 30 days or less  Yes, every 90 days or less  Yes, every 180 days or less  Yes, every 365 days or less  Other (Provide additional comments)  No  Click here to enter text. |
| 3.5 Awareness and Training | | |
| 3.5.1  N/A More | Which of the following applies to security awareness training of staff? *(Select all that apply)* | In-person security training  Mandatory for all staff  Tailored dependent on role  Staff periodically test phished  Online security training material  Staff notices regarding new security threats  Password security best practices training  Other (Provide additional comments)  None of the above  Click here to enter text. |
| 3.5.2  N/A More | Does the company employ a secure password management solution for employees to store passwords? *(Select all that apply)* | Yes, internally and centrally hosted  Yes, cloud-based  Yes, desktop-based (local storage only)  No  Click here to enter text. |
| 3.5.3  N/A More | How often does the company conduct security awareness training? *(Select all that apply)* | On an as-needed basis for individuals  When staff first join  Annually  Other (Provide additional comments)  No training is provided  Click here to enter text. |
| 3.6 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 3.7 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

| 4. Data Security | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 16. | | |
| 4.1 Data Management | | |
| 4.1.1  N/A More | Does the company process Non-Public Personal Information (‘NPPI’) or Personally Identifiable Information (‘PII’) or Sensitive Personal Information (‘SPI’) (whether supplied by the client or other party) as it pertains the product/service offered? | Yes  No |
| 4.1.2  N/A More | Where does the company store client data for this product and/or service? *(Select all that apply)* | Data centers  Cloud providers  On laptops or other devices allowed to be carried offsite by employees  On laptops or other devices not allowed to be carried offsite  On laptops or other devices controlled by contractors  Other (Provide additional comments)  Not applicable  Click here to enter text. |
| 4.1.3  N/A More | If storing or processing multiple clients’ data, how is the data segregated? *(Select all that apply)* | Logically segregated (e.g., within applications)  Virtually segregated infrastructure (e.g., separate VPC or Virtual Machines per client)  Physically segregated infrastructure  No segregation  Not applicable  Other (Provide additional comments)  Click here to enter text. |
| 4.1.4  N/A More | Does the company apply any classification and safeguarding of data according to sensitivity? | Yes  No |
| 4.2 Encryption | | |
| 4.2.1  N/A More | Please indicate all the ways which encryption is used to protect client data at rest. *(Select all that apply)* | Encrypted fields in databases/files  Database/file encryption  Filesystem encryption  Full disk encryption  Encrypted on all removable media (e.g., USB drives)  Encrypted on all portable devices (e.g., laptops)  Other (Provide additional comments)  No encryption used  Not applicable  Click here to enter text. |
| 4.2.2  N/A More | Please indicate all the ways in which encryption is used to protect client data sent via email. *(Select all that apply)* | Encrypted in transport (Enforced TLS)  Encrypted in transport (Opportunistic TLS)  Encrypted attachments (e.g., protected zip files)  End-to-end encryption (e.g., PGP, S/MIME)  Secure web portal  Other (Provide additional comments)  No encryption used  Not applicable  Click here to enter text. |
| 4.2.3  N/A More | Please indicate all the ways in which encryption is used to protect client data exchanged via online file transfer. *(Select all that apply)* | Encrypted in transport (e.g., FTPS, SFTP, HTTPS)  Encrypted files (e.g., PGP, protected zip files)  Other (Provide additional comments)  No encryption used  Not applicable  Click here to enter text. |
| 4.2.4  N/A More | Who has access to the company’s decryption keys? *(Select all that apply)* | IT  IT infrastructure admins  Head of information security  One or more other information security team members  Chief Executive Officer  Chief Technology Officer  Chief Operating Officer  One or more persons who are not employees of the company who are identified below  Other (Provide additional comments)  No encryption used  Click here to enter text. |
| 4.3 Mobile Access | | |
| 4.3.1  N/A More | (a) Does the company allow employees to use company provisioned laptops or tablet devices to store or process company information? | Yes  No, and, as a consequence, (b)-(c) below have been left blank.  No, and, as a consequence, the rows for Questions 4.3.1(b)-(c) in the template DDQ have been omitted. |
| N/A More | (b) What security measures does the company implement to protect information on all company provisioned laptops and tablet devices? *(Select all that apply)* | Antivirus  Configuration management  Data loss prevention  Drive encryption  Endpoint Detection and Response (EDR)  Enforced VPN  Host-based firewall  Host-based Intrusion Prevention System (HIPS)  Inventory management  Location tracking  Mobile device policy  Mobile Device Management (MDM) platform  Operating system hardening  Web filtering  Regular patching schedule (at least quarterly)  Remote wipe capabilities  Sandboxing  Other (Provide additional comments)  None (Provide additional comments)  Click here to enter text. |
| N/A More | (c) Are all employees, consultants and subcontractors subject to the same laptop/tablet security measures? | Yes  No, there are differences or exceptions for certain individuals and an explanation is provided below.  Click here to enter text. |
| 4.3.2  N/A More | (a) Does the company allow employees to use removable media (e.g., USB storage, DVD) to store or process company information? *(Select all that apply)* | Yes  No except as explained below  No, and, as a consequence, (b)-(c) below have been left blank.  No, and, as a consequence, the rows for Questions 4.3.2(b)-(c) in the template DDQ have been omitted.  Click here to enter text. |
| N/A More | (b) Is this set out solely as employee policy or is it enforced via software and/or hardware? *(Select all that apply)* | Written policy only  Enforced using software  Enforced using hardware  Other (Provide additional comments)  None of the above (Provide additional comments)  Click here to enter text. |
| N/A More | (c) What security measures does the company implement to protect information on all removable media and the devices the media is plugged into? *(Select all that apply)* | Antivirus  Configuration management  Data loss prevention  Endpoint Detection and Response (EDR)  Enforced encryption of removable media  Host-based firewall  Host-based Intrusion Prevention System (HIPS)  Regular patching schedule (at least quarterly)  Inventory management  Other (Provide additional comments)  None (Provide additional comments)  Click here to enter text. |
| 4.3.3  N/A More | (a) Does the company allow employees to use company provisioned mobile devices to store or process company information? *(Select all that apply)* | Yes  No, and, as a consequence, (b)-(c) below have been left blank.  No, and, as a consequence, the rows for Questions 4.3.3(b)-(c) in the template DDQ have been omitted. |
| N/A More | (b) What security measures does the company implement to protect information on all company provisioned mobile devices? *(Select all that apply)* | Application whitelisting  Disallow jail-broken/rooted devices  Encryption of all storage  Enforced patch levels  Enforced VPN  Inventory management  Location tracking  Mobile device policy  Mobile Device Management (MDM) platform  Multifactor authentication  Remote wipe capabilities  Secure containers  Strong PIN/password protection  Other (Provide additional comments)  None (Provide additional comments)  Click here to enter text. |
| N/A More | (c) Are all employees, consultants and subcontractors subject to the same company provisioned mobile device security measures? | Yes  No, there are differences or exceptions for certain individuals and an explanation is provided below.  Click here to enter text. |
| 4.3.4  N/A More | (a) Does the company allow employees to bring their own mobile devices (i.e., BYOD) to store or process company information? | Yes  No, and, as a consequence, (b)-(c) below have been left blank.  No, and, as a consequence, the rows for Questions 4.3.4(b)-(c) in the template DDQ have been omitted. |
| N/A More | (b) What safeguards does the company have in place to prevent staff’s personal devices from being compromised? *(Select all that apply)* | Application whitelisting  BYOD policy  Disallow jail-broken/rooted devices  Encryption of all storage  Enforced patch levels  Enforced VPN  Inventory management  Location tracking  Mobile Device Management (MDM) platform  Multifactor authentication  Remote wipe capabilities  Secure containers  Strong PIN/password protection  Other (Provide additional comments)  None (Provide additional comments)  Click here to enter text. |
| N/A More | (c) Are all employees, consultants and subcontractors subject to the same personal mobile device security measures? | Yes  No, there are differences or exceptions for certain individuals and an explanation is provided below.  Click here to enter text. |
| 4.4 Data Loss Prevention | | |
| 4.4.1  N/A More | Does the company have monitoring to prevent or detect data leakage? | Yes, and details are provided below.  No  Click here to enter text. |
| 4.4.2  N/A More | Please indicate the types of sites/services blocked by the company through a web proxy or other means. *(Select all that apply)* | Compromised/malicious web sites  Personal web mail  Data sharing sites  Social media sites  Internet chat  Other (Provide additional comments)  No services are blocked  Click here to enter text. |
| 4.4.3  N/A More | Which of the following applies to the secure disposal of electronic storage media (e.g., hard drives, optical media) and hard copy data (e.g., document pulping or shredding)? *(Select all that apply)* | Store physical devices in a location with restricted access  Maintain records of decommissioning  Obtain evidence (Certificate of Disposal)  Secure removal and destruction of documents based on sensitivity of data  Secure removal and destruction of electronic storage media based on sensitivity of data  Other (Provide additional comments)  None (Provide additional comments)  Click here to enter text. |
| 4.5 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 4.6 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

| 5. System Maintenance | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 19. | | |
| 5.1 Asset Management | | |
| 5.1.1  N/A More | (a) Does the company keep an inventory of physical hardware and virtual assets? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 5.1.1(b) in the template DDQ has been omitted. |
| N/A More | (b) How often is the inventory of physical hardware and virtual assets reviewed and updated? *(Select all that apply)* | Upon the initial provisioning and final destruction and disposal of the asset  Annually  Semi-annually  Quarterly  Monthly  Weekly  Daily  Continuously as changes are made  Other (Provide additional comments)  Never  Click here to enter text. |
| 5.1.2  N/A More | (a) Does the company keep an inventory of software applications in use? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 5.1.2(b) in the template DDQ has been omitted. |
| N/A More | (b) How often is the inventory of software applications reviewed and updated? *(Select all that apply)* | Upon the initial installation and removal of the software  Annually  Semi-annually  Quarterly  Monthly  Weekly  Daily  Continuously as changes are made  Other (Provide additional comments)  Never  Click here to enter text. |
| 5.1.3  N/A More | (a) Does the company keep a record of the network architecture/topology? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 5.1.3(b) in the template DDQ has been omitted. |
| N/A More | (b) How often is the network architecture/topology reviewed and updated? *(Select all that apply)* | Upon the initial setup and decommissioning of a network device  Annually  Semi-annually  Quarterly  Monthly  Weekly  Daily  Continuously as changes are made  Other (Provide additional comments)  Never  Click here to enter text. |
| 5.2 Process | | |
| 5.2.1  N/A More | What testing is performed before applying major third-party system updates? *(Select all that apply)* | Tested by technical staff  Tested by end users  Automated testing  Rollback plans are made and tested  Deployed into a separate test environment  Security review  Performance and capacity review  Other (Provide additional comments)  None (Provide additional comments)  Click here to enter text. |
| 5.2.2  N/A More | Does the company provide advanced notification to all affected business units prior to performing system upgrades or maintenance? | Yes  No |
| 5.2.3  N/A More | (a) Does the company conduct regular vulnerability assessments on its internal devices? | Yes  No, and, as a consequence, (b)-(c) below have been left blank.  No, and, as a consequence, the rows for Questions 5.2.3(b)-(c) in the template DDQ have been omitted.  Not applicable, and, as a consequence, (b)-(c) below have been left blank.  Not applicable, and, as a consequence, the rows for Questions 5.2.3(b)-(c) in the template DDQ have been omitted. |
| N/A More | (b) How often does the company conduct a vulnerability assessment? *(Select one)* | Intraday  At least daily  At least weekly  At least monthly  At least quarterly  At least semi-annually  At least annually  Other (Provide additional comments)  Click here to enter text. |
| N/A More | (c) Which of the following does the company check as part of the vulnerability assessments performed? *(Select all that apply)* | All computers  All workstations  All servers  All printers, telephones and network devices  All internet facing systems  Missing operating system patches  Out of date software  Web application vulnerabilities  Fuzzing  Other (Provide additional comments)  Click here to enter text. |
| 5.2.4  N/A More | (a) How often are security updates applied to all network devices, servers, desktops and applications? *(Select all that apply)* | Daily  Weekly  Monthly  Quarterly  Semi-annually  Annually  Other (Provide additional comments)  Never  Not applicable, and, as a consequence, (b) below has been left blank.  Not applicable, and, as a consequence, the row for Question 5.2.4(b) in the template DDQ has been omitted.  Click here to enter text. |
| N/A More | (b) In the event that critical vulnerabilities are found on any network device, server, desktop or application, is there a process to review the risk posed and patch the vulnerability outside of the normal schedule if required? | Yes  No |
| 5.2.5  N/A More | How does the company stay up-to-date with new vulnerabilities and other security risks? *(Select all that apply)* | Vulnerability scanner feed updates  Product subscriptions to IOC feeds (e.g., STIX/TAXII)  Personal/group subscriptions to vulnerability feeds  Review of/subscriptions to product release notes  Cyber security news feeds or online forums  Private threat intelligence forums  Attending industry/community events  Peer-to-peer information sharing groups  Periodic discussions with red teams  Other (Provide additional comments)  Click here to enter text. |
| 5.3 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 5.4 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

| 6. Access Controls | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 23. | | |
| 6.1 Entitlements | | |
| 6.1.1  N/A More | Are entitlements to all applications, databases, servers and systems restricted only to personnel who need such access for operational purposes (i.e., least privilege)? | Yes  No |
| 6.1.2  N/A More | How often are the user entitlements to all applications, databases, servers and systems reviewed? *(Select all that apply)* | On initial setup only  Daily  Weekly  Monthly  Quarterly  Semi-annually  Annually  Other (Provide additional comments)  Never  Click here to enter text. |
| 6.1.3  N/A More | With the exception of break glass access through a privileged account management system, is the use of shared user IDs strictly prohibited? | Yes  No, and details are provided below.  Click here to enter text. |
| 6.2 Client Access Controls | | |
| 6.2.1  N/A More | (a) Does the company provide clients a login of any type? | Yes  No, and, as a consequence, (b)-(n) below have been left blank.  No, and, as a consequence, the rows for Questions 6.1.2(b)-(n) in the template DDQ have been omitted. |
| N/A More | (b) Are client logon credentials (user ID and password) encrypted during network transit? | Yes  No |
| N/A More | (c) Are client passwords protected in storage (i.e., using a securely designed password hashing function)? | Yes, and details are provided below.  No  Click here to enter text. |
| N/A More | (d) Is there an automated control in place to prevent excessive login attempts under the same account or from the same IP address (i.e., client accounts will be locked after a predefined number of unsuccessful login attempts)? | Yes, and details are provided below.  No  Click here to enter text. |
| N/A More | (e) Can a client change his/her own password? | Yes, and details on the min/max password length and complexity requirements are below.  No  Click here to enter text. |
| N/A More | (f) Does the company’s system log clients off after a predefined period of inactivity? | Yes, and details are provided below.  No  Click here to enter text. |
| N/A More | (g) Are passwords always entered in a masked-entry field (e.g., masked with an asterisk ‘\*’ as user type)? | Yes  No |
| N/A More | (h) Are login attempts logged with a date, time, user ID and source network address? *(Select one)* | Yes, all login attempts logged with a date, time, user ID and source network address.  Yes, all login attempts logged, and the information logged is discussed below.  Yes, some login attempts logged with a date, time, user ID and source network address and the types of login attempts that are logged and the types that are not logged are described below.  Yes, some login attempts logged. The types of login attempts that are logged and the types that are not logged, along with a description of the information logged, are discussed below.  No. Login attempts are not logged at all.  Click here to enter text. |
| N/A More | (i) For how long are logs of attempted logins retained? *(Select one)* | At least one day  At least a week  At least a month  At least a year  Other (Provide additional comments)  No such logs are retained  Click here to enter text. |
| N/A More | (j) Does the company’s system support single sign on (SSO) methods for authentication? | Yes, and details are provided below.  No  Click here to enter text. |
| N/A More | (k) Does the company’s system offer the ability to restrict access within the application based on roles assigned to authorized users? | Yes, and details are provided below.  No  Click here to enter text. |
| N/A More | (l) Does the company’s system provide security reports that identify users and their specific entitlements for periodic review? | Yes  No |
| N/A More | (m) Does the company’s system provide access audit reports for client review? | Yes  No |
| N/A More | (n) Does the company’s system support multi-factor authentication (MFA) for client logins? | Yes  No |
| 6.2.2  N/A More | (a) Can company employees login as a client user (e.g., emulation)? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 6.2.2(b) in the template DDQ has been omitted. |
| N/A More | (b) Is this action captured in the audit log? | Yes  No |
| 6.2.3  N/A More | Can access to the company’s systems be restricted to only the client’s public IP ranges? | Yes  No |
| 6.3 Internal Staff Access Controls | | |
| 6.3.1  N/A More | Which of the following applies to the use of two-factor authentication within the company? *(Select all that apply)* | Used for all remote access by staff  Used for all logins internally  Used for access to restricted administrative functions/high risk environments/elevated rights  Other (Provide additional comments)  Not applicable  Click here to enter text. |
| 6.3.2  N/A More | Which of the following applies to granting, denying and reviewing the authorization and entitlements to company resources? *(Select all that apply)* | Entitlements are approved by business sponsor/manager  Entitlements are reviewed periodically for appropriateness  Entitlements are reviewed upon role changes/termination  Entitlements are centrally managed by a restricted group of administrators  Entitlements process follows a role-based access approach  Entitlements follow the principle of least privilege  Other (Provide additional comments)  Not applicable  Click here to enter text. |
| 6.3.3  N/A More | Which of the following controls apply to remote access for company staff? *(Select all that apply)* | Users are prevented from copying data to/from the remote computer  Users are prevented from printing  Other (Provide additional comments)  Not applicable  Click here to enter text. |
| 6.3.4  N/A More | (a) Which of the following applies as it pertains to the logging of staff activity when accessing client data? *(Select all that apply)* | Logs are aggregated and stored centrally for analysis and review  Logs are stored directly on the systems accessed  Logs are reviewed on a regular basis for anomalies  Alerts are generated from anomalies discovered in logs  Logs are secured to protect against alteration  No logging of this activity, and, as a consequence, (b)-(d) below have been left blank.  No logging of this activity, and, as a consequence, the rows for Questions 6.3.4(b)-(d) in the template DDQ have been omitted. |
| N/A More | (b) How long are activity logs retained for? *(Select one)* | At least one day  At least a week  At least a month  At least a year  Other (Provide additional comments)  Click here to enter text. |
| N/A More | (c) What information is recorded within the log data to support forensic investigation? *(Select all that apply)* | Event source  Date and time  Source addresses  Destination addresses  Records/context accessed or modified  Network requests/traffic  Commands executed/actions taken  User  Other (Provide additional comments)  Click here to enter text. |
| N/A More | (d) Is there any type of “super user” or “ghost” account whose access is not captured by the audit log? | Yes  No |
| 6.4 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 6.5 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

| 7. Infrastructure Security | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 27. | | |
| 7.1 Network Security | | |
| 7.1.1  N/A More | Which of the following applies to the network protection(s) in place? *(Select all that apply)* | Firewalls  Port security  Intrusion Prevention System (IPS)  Intrusion Detection System (IDS)  Anomaly monitoring  DHCP snooping  Dynamic ARP Inspection (DAI)  Honeypots  Other (Provide additional comments)  No network security solution is in place  Click here to enter text. |
| 7.1.2  N/A More | (a) Which of the following applies as it pertains to the logging of system activity and network traffic? *(Select all that apply)* | Logs are aggregated and stored centrally for analysis and review  Logs are stored directly on the systems accessed  Logs are reviewed on a regular basis for anomalies  Alerts are generated from anomalies discovered in logs  Logs are secured to protect against alteration  No logging of this activity, and, as a consequence, (b)-(d) below have been left blank.  No logging of this activity, and, as a consequence, the rows for Questions 7.1.2(b)-(d) in the template DDQ have been omitted. |
| N/A More | (b) How long are activity logs retained for? *(Select one)* | At least one day  At least a week  At least a month  At least a year  Other (Provide additional comments)  Click here to enter text. |
| N/A More | (c) What type of logs are aggregated and stored centrally? *(Select all that apply)* | DNS  Firewall  IDS/IPS  Network devices (e.g., routers, switches)  Endpoint security logs  Operating system events  E-mail traffic  Application logs  Web logs  Filesystem accesses  Other (Provide additional comments)  None  Click here to enter text. |
| N/A More | (d) What information is recorded within the log data to support forensic investigation? *(Select all that apply)* | Event source  Date and time  Source addresses  Destination addresses  Records/context accessed or modified  Network requests/traffic  Commands executed/actions taken  User  Other (Provide additional comments)  Click here to enter text. |
| 7.1.3  N/A More | Does the company enforce multi-factor authentication (MFA) when all internal staff, contractors and consultants connect remotely (e.g., through a VPN, external web access, Outlook Web Access or other)? | Yes  No  Not applicable |
| 7.1.4  N/A More | Which of the following methods are used to mitigate Distributed Denial of Service (DDoS) attacks on the company? *(Select all that apply)* | Network scrubbing centers  Protocol inspection/blocking  Human challenges  Other (Provide additional comments)  None  Not applicable  Click here to enter text. |
| 7.1.5  N/A More | Does the company monitor for unauthorized network connection points such as wireless access points, modems, etc.? | Yes  No  Not applicable |
| 7.1.6  N/A More | Is a solution in place to protect company email against spam and malware? | Yes  No |
| 7.1.7  N/A More | (a) Does the company’s platform or service require connecting to a client’s network or servers? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 7.1.7(b) in the template DDQ has been omitted. |
| N/A More | (b) Is any client data copied or cached within the company’s infrastructure? | Yes, and details are provided below.  No  Click here to enter text. |
| 7.2 Endpoint Security | | |
| 7.2.1  N/A More | Which of the following applies to the endpoint protection(s) in place? *(Select all that apply)* | Endpoint Protection Platform (EPP)  Endpoint Detection & Response (EDR)  Antimalware  Antivirus  Application whitelisting  Data loss prevention (DLP)  Endpoint firewall  Operating System exploit mitigations  Disabling unneeded Operating System functionality (e.g., NBT-NS, LLMNR)  Microsoft Office macro prevention  Host-based Intrusion Prevention System (HIPS)  Other (Provide additional comments)  No endpoint security solution is in place  Click here to enter text. |
| 7.2.2  N/A More | Does the company have endpoint protection installed on all servers and workstations? | Yes  No, and details as to why not (or exceptions) are provided below.  Click here to enter text. |
| 7.2.3  N/A More | Does the company restrict administrative access to desktops, laptops, phones and tablets for all employees and third parties? | Yes  No, and details are provided below.  Not applicable  Click here to enter text. |
| 7.3 Penetration Testing | | |
| 7.3.1  N/A More | (a) Does the company conduct periodic penetration tests on its external facing applications, network and devices? | Yes  No, and, as a consequence, (b)-(c) below have been left blank.  No, and, as a consequence, the rows for Questions 7.3.1(b)-(c) in the template DDQ have been omitted.  Not applicable, and, as a consequence, (b)-(c) below have been left blank.  Not applicable, and, as a consequence, the rows for Questions 7.3.1(b)-(c) in the template DDQ have been omitted. |
| N/A More | (b) How often does the company conduct a penetration test? *(Select all that apply)* | Continuously, we have an ongoing red team contract  On every significant technology change  On every significant internet-facing technology change  At least semi-annually  At least annually  Other (Provide additional comments)  Click here to enter text. |
| N/A More | (c) Which of the following does the company include as part of the penetration test scope? *(Select all that apply)* | All workstations  All servers  All internet facing systems  A representative subset of the environment  Infrastructure assessment  Application assessment  Other (Provide additional comments)  Click here to enter text. |
| 7.4 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 7.5 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

| 8. Physical Security | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 31. | | |
| 8.1 Office Access Security | | |
| 8.1.1  N/A More | Have steps been taken to ensure that only authorized personnel are able to physically access critical computer systems? | Yes, and details are provided below.  No  Click here to enter text. |
| 8.1.2  N/A More | (a) What type of entry access control system does the company utilize at each office? *(Select all that apply)* | Biometric  Key card  Combination lock  Physical key  Other (Provide additional comments)  The company does not use an entry access control system, and, as a consequence, (b)-(d) below have been left blank.  The company does not use an entry access control system, and, as a consequence, the rows for Questions 8.1.2(b)-(d) in the template DDQ have been omitted.  Click here to enter text. |
| N/A More | (b) Does the company’s entry access control system at each office generate an entry log? | Yes  No, and, as a consequence, (c)-(d) below have been left blank.  No, and, as a consequence, the rows for Questions 8.1.2(c)-(d) in the template DDQ have been omitted. |
| N/A More | (c) For how long are the entry records into each of the company’s offices retained? *(Select one)* | At least one day  At least a week  At least a month  At least three months  At least six months  At least a year  Other (Provide additional comments)  The entry records are not retained.  Click here to enter text. |
| N/A More | (d) How often are the entry logs reviewed or audited? *(Select all that apply)* | On-demand, only when required.  Daily  Weekly  Monthly  Quarterly  Semi-annually  Annually  Other (Provide additional comments)  Never  Click here to enter text. |
| 8.1.3  N/A More | (a) Does the company use a video surveillance system to monitor their premises? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 8.1.3(b) in the template DDQ has been omitted. |
| N/A More | (b) For how long are the recordings from the video surveillance system retained? (*Select one*) | At least one day  At least a week  At least a month  At least three months  At least six months  At least a year  Other (Provide additional comments)  No recordings are retained  Click here to enter text. |
| 8.1.4  N/A More | (a) Are procedures in place to manage visitors within the office? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 8.1.4(b) in the template DDQ has been omitted. |
| N/A More | (b) Have steps been taken to ensure visitors do not have the ability to observe or access employee computer systems or confidential information? | Yes, and details are provided below.  No  Click here to enter text. |
| 8.1.5  N/A More | Does the company enforce automatic screen-locking on all workstations after a specified period of inactivity? | Yes, and details are provided below.  No  Click here to enter text. |
| 8.2 Server Access Security | | |
| 8.2.1  N/A More | (a) What type of access control system does the company use to protect its data center(s), communications room(s) and/or server room(s)? *(Select all that apply)* | Biometric  Key card  Combination lock  Physical key  Other (Provide additional comments)  The company does not use an access control system for any of its data center(s), communications room(s) and server room(s), and, as a consequence, (b)-(c) below have been left blank.  The company does not use an access control system for any of its data center(s), communications room(s) and server room(s), and, as a consequence, the rows for Questions 8.2.1(b)-(c) in the template DDQ have been omitted.  Click here to enter text. |
| N/A More | (b) Does the company’s access control system protecting its data center(s), communications room(s) and/or server room(s) generate an entry log? | Yes  No, and, as a consequence, (c) below has been left blank.  No, and, as a consequence, the row for Question 8.2.1(c) in the template DDQ has been omitted. |
| N/A More | (c) For how long are the entry records into each of the company’s its data center(s), communications room(s) and/or server room(s) retained? *(Select one)* | At least one day  At least a week  At least a month  At least three months  At least six months  At least a year  Other (Provide additional comments)  The entry records are not retained  Click here to enter text. |
| 8.2.2  N/A More | Please provide details on who has access to the datacenter(s), communications and/or server room(s). | Click here to enter text. |
| 8.2.3  N/A More | Please provide details on how an individual’s access is granted to or revoked from datacenter(s), communication and/or server room(s), and how often access lists are reviewed. | Click here to enter text. |
| 8.2.4  N/A More | Do the facilities that provide services to clients have manned security guarding them? | Yes, and details are provided below.  No  Click here to enter text. |
| 8.2.5  N/A More | Is the company able to remotely monitor and record its hardware within its datacenter(s) via closed-circuit television (CCTV)? | Yes, and details are provided below.  No  Click here to enter text. |
| 8.3 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 8.4 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

| 9. Business Continuity | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 35. | | |
| 9.1 Policy | | |
| 9.1.1  N/A More | (a) Has the company developed a Business Continuity Plan (BCP)? | Yes  No, and, as a consequence, (b)-(f) below have been left blank.  No, and, as a consequence, the rows for Questions 9.1.1(b)-(f) in the template DDQ have been omitted. |
| N/A More | (b) Is it formally documented? | Yes  No |
| N/A More | (c) Is the plan reviewed on a periodic basis to determine if the controls are operating as intended? | Yes  No |
| N/A More | (d) How frequently is the plan reviewed for appropriateness and updated as necessary? *(Select one)* | At least daily  At least weekly  At least monthly  At least quarterly  At least semi-annually  At least annually  Other (Provide additional comments)  Never  Click here to enter text. |
| N/A More | (e) Does the plan address whether the company has sufficient system redundancy to ensure reasonable protection in the event of a disaster or system failure? | Yes  No |
| N/A More | (f) Does the plan have any specific provisions to address the more common types of cyber attacks encountered? | Yes  No |
| 9.1.2  N/A More | Does the company have a vendor risk management process in place to assess the risk and resilience of critical third parties the company depends on? | Yes, and details are provided below.  No  Click here to enter text. |
| 9.2 Specifications | | |
| 9.2.1  N/A More | What type of data centers does the company use? *(Select all that apply)* | On premises  Fully-owned datacenter  Private cloud from a vendor  Public cloud (e.g., IaaS, PaaS, FaaS)  SaaS (Software as a Service such as Google docs, Office 365, Salesforce)  Other (Provide additional comments)  None  Click here to enter text. |
| 9.2.2  N/A More | Has a secondary location been established for staff to work in the event of a disaster or system failure? | Yes, and details are provided below.  No  Click here to enter text. |
| 9.2.3  N/A More | Do the company’s servers and network devices receive power from sources backed with battery and/or generator power with sufficient surge protection? | Yes  No |
| 9.2.4  N/A More | Please select the option closest to the company’s set expected Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for failover to backup systems. *(Select one)* | Same day recovery with data up to the point of failure  Same day recovery with data from the previous day  Next day recovery with data up to the point of failure  Other (Provide additional comments)  No specific RTO/RPO set  Click here to enter text. |
| 9.2.5  N/A More | Were the RTO and RPO met during the most recent test of the BCP? | Yes, and details are provided below.  No, and details are provided below.  Not applicable  Click here to enter text. |
| 9.2.6  N/A More | (a) Has the company configured appropriate retention polices for all system backups? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 9.2.6(b) in the template DDQ has been omitted. |
| N/A More | (b) Is critical systems data archived long enough to comply with relevant industry regulations? | Yes  No |
| 9.2.7  N/A More | (a) How frequently are BCP/DR tests performed? *(Select one)* | At least monthly  At least quarterly  At least semi-annually  At least annually  Other (Provide additional comments)  Never, and, as a consequence, (b) below has been left blank.  Never, and, as a consequence, the row for Question 9.2.7(b) in the template DDQ has been omitted.  Click here to enter text. |
| N/A More | (b) Which elements of the company’s estate are tested as part of its BCP/DR testing program? *(Select all that apply)* | System and data recovery  Data center failover  Workplace recovery  Communications infrastructure  Staff call tree or notification system  Cyber defense and incident detection capabilities  Other (Provide additional comments)  Click here to enter text. |
| 9.2.8  N/A More | At what interval does the company perform test restores from backups containing critical systems data to ensure the integrity of the backup procedures and data? *(Select one)* | At least daily  At least weekly  At least monthly  At least quarterly  At least semi-annually  At least annually  Other (Provide additional comments)  Never  Click here to enter text. |
| 9.2.9  N/A More | Have training procedures and documentation been established at the company to ensure all employees clearly understand the BCP? | Yes  No |
| 9.2.10  N/A More | Are dedicated cooling and fire suppression systems in place to protect against system interruptions? | Yes  No |
| 9.2.11  N/A More | (a) Has the company established a secondary location to retain backup copies of all critical client and company data? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 9.2.11(b) in the template DDQ has been omitted. |
| N/A More | (b) At what frequency is critical data copied to a secondary location? *(Select one)* | Continuously (near real-time)  Within an hour  Hourly  Daily  Weekly  Other (Provide additional comments)  Critical data is not copied offsite  Click here to enter text. |
| 9.2.12  N/A More | Which of the following methods are used for backing up critical systems and data? *(Select all that apply)* | Site to site *synchronous* replication  Site to site *asynchronous* replication  Storage snapshots  Object store backup  Cloud backup  Removeable backup media  Other (Provide additional comments)  Critical systems and data are not backed up  Click here to enter text. |
| 9.2.13  N/A More | Are backups containing client data encrypted both in transit and while at rest? *(Select one)* | In transit only  At rest only  Both in transit and at rest  Other (Provide additional comments)  Neither in transit nor at rest  Click here to enter text. |
| 9.2.14  N/A More | If backups are physically transferred, is it done by authorized couriers in protected vehicles and stored in protected and professional storage facilities? | Yes  No, and details are provided below.  Not applicable  Click here to enter text. |
| 9.2.15  N/A More | Please select the option that most closely describes the capacity of the company’s infrastructure in the event of a BCP/DR incident involving critical systems and data. *(Select one)* | Operates at or near normal production capacity for a sustained period  Operates at a reduced capacity or for a limited duration, and a further explanation is provided below.  Other (Provide additional comments)  Click here to enter text. |
| 9.2.16  N/A More | Has the BCP/DR plan been activated in the past three years? | Yes, and details are provided below.  No  Click here to enter text. |
| 9.2.17  N/A More | Were the RPOs and RTOs met in all instances where the BCP/DR plan had been activated? | Yes  No, and details are provided below.  The BCP/DR plan has never been activated.  Click here to enter text. |
| 9.3 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 9.4 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

| 10. Cyber Incident Response | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 38. | | |
| 10.1 Cyber Incident Response Plan | | |
| 10.1.1  N/A More | Has the company developed a formal, documented Cyber Incident Response Plan (CIRP) that describes workflow in the event of a cyber incident? | Yes  No  Click here to enter text. |
| 10.1.2  N/A More | Is the Cyber Incident Response Plan reviewed on a periodic basis to determine if the controls are operating as intended? | Yes  No |
| 10.1.3  N/A More | Does the company have a retainer/master services agreement in place with an incident response services provider? | Yes  No  Click here to enter text. |
| 10.2 Detection and Response | | |
| 10.2.1  N/A More | How regularly are systems, logs and events monitored for evidence of a cyber security incident? *(Select all that apply)* | Alerts are reviewed continuously in (near) real-time  When a user reports a potential problem  Daily  Intraweek  Weekly  Monthly  Quarterly  Semi-annually  Annually  Other (Provide additional comments)  Not regularly monitored  Click here to enter text. |
| 10.2.2  N/A More | Is an alerting mechanism in place to notify staff of IT related incidents? | Yes  No |
| 10.2.3  N/A More | If a cyber incident is detected, what team(s) or individual(s) lead the response? *(Select all that apply)* | IT helpdesk  Managed security service provider  Dedicated security operations team  Dedicated security team  IT team  Pre-determined incident response team  Other (Provide additional comments)  Click here to enter text. |
| 10.2.4  N/A More | Is the company a member of an information sharing initiative such as an ISAC, the UK Cybersecurity Information Sharing Partnership (CiSP), the Canadian Cyber Incident Response Center (CCIRC) or similar? | Yes, and details are provided below.  No  Click here to enter text. |
| 10.3 Cyber Incidents | | |
| 10.3.1  N/A More | (a) Has the company experienced any material internal or external information security incident in the past three years? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 10.3.1(b) in the template DDQ has been omitted. |
| N/A More | (b) Please describe any incidents, lessons-learned and solutions put in place to mitigate a repeat of that type of incident going forward. | Click here to enter text. |
| 10.3.2  N/A More | Has the company experienced any non-material internal or external information security incident in the past 12 months? | Yes, and a description is provided below.  No  Click here to enter text. |
| 10.3.3  N/A More | (a) Has the company been made aware of any material internal or external information security incident involving one of their subcontractors or service providers in the past three years? | Yes  No, and, as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 10.3.3(b) in the template DDQ has been omitted. |
| N/A More | (b) Please describe the incidents, lessons-learned and solutions put in place to mitigate a repeat of that type of incident going forward. | Click here to enter text. |
| 10.4 Client Notification | | |
| 10.4.1  N/A More | Does the company have policies in place that detail when clients and relevant providers in its supply chain should be alerted to security or IT incidents that have impacted the company? | Yes, and a description of the process used to determine when a client should be notified is provided below.  No  Not applicable  Click here to enter text. |
| 10.4.2  N/A More | How are clients notified of security or IT incidents? *(Select all that apply)* | Email  Telephone call  Text message  Posting on the company’s website  Other (Provide additional comments)  No notification mechanism is in place  Not applicable  Click here to enter text. |
| 10.4.3  N/A More | In what timeframe does the company endeavor to notify clients of security incidents? *(Select one)* | Less than one business day  1-2 business days  3-5 business days  More than a week  Not applicable  No specific service level is offered, and further details as to why are available in the comments below.  Click here to enter text. |
| 10.5 Cybersecurity Insurance | | |
| 10.5.1  N/A More | (a) Does the company have cybersecurity insurance? | Yes  No, and, as a consequence, the rest of this section has been left blank and an explanation of why no cybersecurity insurance has been purchased is provided below.  No, and, as a consequence, the rows for Questions 10.5.1(b)-(d) in the template DDQ have been omitted and an explanation of why no cybersecurity insurance has been purchased is provided below.  Click here to enter text. |
| N/A More | (b) What is the liability limit for the company’s cybersecurity insurance? | Click here to enter text. |
| N/A More | (c) What does the company’s cybersecurity insurance cover (e.g., forensics, defense costs, cyber extortion payments)? | Click here to enter text. |
| N/A More | (d) Has the company ever made a claim on the cybersecurity insurance policy? | Yes, and details are provided below.  No  Click here to enter text. |
| 10.6 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 10.7 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

| 11. Software Development | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 40. | | |
| 11.1 In-House Development Practices | | |
| 11.1.1  N/A More | Does the company do any in-house software development or is the company the recipient of custom software developed by a third party on their behalf? | Yes  No, and, as a consequence, the rest of this section has been left blank.  No, and, as a consequence, the rows for Questions 11.1.2-11.1.13 in the template DDQ have been omitted. |
| 11.1.2  N/A More | Is source code escrowed with a third party? | Yes, and the third party holding the source code is detailed below.  No  Click here to enter text. |
| 11.1.3  N/A More | Are separate environments maintained for development, testing and production? | Yes  No, and details are provided below.  Click here to enter text. |
| 11.1.4  N/A More | Does the company offer their development staff specific security training related to common vulnerabilities (e.g., OWASP top 10)? | Yes, and details are provided below.  No  Click here to enter text. |
| 11.1.5  N/A More | Which of the following types of testing does the company perform? *(Select all that apply)* | Unit testing  Integration testing  Regression testing  Static security testing  Dynamic security testing  User acceptance testing  Other (Provide additional comments)  None  Click here to enter text. |
| 11.1.6  N/A More | Does the company make use of any Continuous Integration and Continuous Delivery practices? | Yes  No |
| 11.1.7  N/A More | Does the company supply release notes with each new software version deployed? | Yes  No |
| 11.1.8  N/A More | Does the company store software in a version control system? | Yes, and the version control system(s) used is detailed below.  No  Click here to enter text. |
| 11.1.9  N/A More | Does the company prevent client data from being used in non-production environments and systems unless obfuscated or scrambled? | Yes  No |
| 11.1.10  N/A More | Has a manual or automated review of the application source code been carried out for internet facing applications, including where the development has been outsourced? | Yes  No  Not applicable |
| 11.1.11  N/A More | Are developers restricted from having access to the production environment? | Yes  No  Other (Provide additional comments)  Click here to enter text. |
| 11.1.12  N/A More | Are application changes tested by staff other than developers prior to implementation? | Yes  No  Other (Provide additional comments)  Click here to enter text. |
| 11.1.13  N/A More | On what frequency are the releases made? *(Select one)* | Intraday  Daily  Intraweek  Weekly  Fortnightly  Monthly  Quarterly  Semi-annually  Annually  Other (Provide additional comments)  Not applicable  Click here to enter text. |
| 11.2 Outsourced Development Practices | | |
| 11.2.1  N/A More | (a) Does the vendor employ any outsourced software development services/partners? | Yes, and the details are provided below  No, and as a consequence, (b) below has been left blank.  No, and, as a consequence, the row for Question 11.2.1(b) in the template DDQ has been omitted.  Click here to enter text. |
| N/A More | (b) Does the company have a full copy of the vendor’s source code? | Yes, and the details of how that copy is updated and transferred are provided below  No  Click here to enter text. |
| 11.3 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 11.4 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

| 12. Vendor Due Diligence by the Company | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 41. | | |
| 12.1 Outsourcing | | |
| 12.1.1  N/A More | (a) Does the company make use of any subcontractors or service providers in providing the relevant product and/or service? | Yes, and the main subcontractors the company uses in relation to the relevant product and/or service are identified below.  No, and, as a consequence, (b)-(c) below have been left blank.  No, and, as a consequence, the rows for Questions 12.1.1(b)-(c) in the template DDQ have been omitted.  Click here to enter text. |
| N/A More | (b) Are any of the subcontractor/service provider product(s) and/or service(s) used hosted in the cloud? | Yes, and details are provided below.  No  Click here to enter text. |
| N/A More | (c) Do the company’s subcontractors/service providers store or process client confidential information? | Yes  No |
| N/A More | (d) Are subcontractors/service providers held to the same level of policy and cybersecurity as company? | Yes  No |
| 12.1.2  N/A More | Does the company perform due diligence on their current and potential subcontractors and service providers? | Yes, and the due diligence process performed is described below.  No  Click here to enter text. |
| 12.2 Service Levels | | |
| 12.2.1  N/A More | Has the company established written Service Level Agreements (SLAs) with service providers and technology partners to help guarantee a stable computing environment? | Yes  No |
| 12.2.2  N/A More | Has the company purchased maintenance contracts with equipment vendors to provide replacement parts in the event of system failure? | Yes  No |
| 12.2.3  N/A More | For critical production systems, has the company established a policy or purchased redundant components to expedite recovery in the event of a failure? | Yes, and details are provided below.  No  Click here to enter text. |
| 12.2.4  N/A More | Please detail the specific security-related contractual provisions the company aims to include in agreements with technology vendors or vendors processing sensitive data. | Click here to enter text. |
| 12.3 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 12.4 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

| 13. Further Information: Critical Outsourced Functions | | |
| --- | --- | --- |
| *To the reader*: In the first column, if the “N/A” box is selected, the company believes the question is not applicable to the company’s operations and the company has deliberately left all of the answer choices for that question blank. If the “More” box is selected, this is a signal to the reader that the company has provided additional information relating to that particular question/response/topic in the “Company Comments” area relevant to this section starting on page 44. | | |
| 13.1 Structure | | |
| 13.1.1  N/A More | Company organization chart (corporate structure), including parent entities and all affiliates providing services to the company’s clients as well as any individuals that directly or indirectly own or control 25% of the outstanding equity of the company (or its parent entity). | Attached/included: Click here to enter text.  Available for review onsite  Available on request: Click here to enter text.  Available online: Click here to enter text.  Not available for review  We do not have one |
| 13.1.2  N/A More | Does the company have any diversity/inclusion certifications? | Yes, and these are identified below.  No  Click here to enter text. |
| 13.2 Further Regulatory and Financial Matters | | |
| 13.2.1  N/A More | Has the company or any member of its senior management ever been convicted of or plead guilty or no contest to an offence or otherwise been conclusively found by any court, regulatory authority or any official body to have engaged in any wrongdoing involving (i) fraud, false or materially misleading statements or omissions, dishonesty, bad faith, willful default; (ii) investments or an investment-related or other financial business; (iii) theft; (iv) bribery, forgery, counterfeiting, extortion or gambling; (v) tax evasion; or (vi) any other felony or misdemeanor (excluding driving offences)?  Please include historical or pending items as part of the response. | Attached/included: Click here to enter text.  Available on request: Click here to enter text.  No  Click here to enter text. |
| 13.2.2  N/A More | Has any application for registration, authorization or a license of any kind to a regulatory body on behalf of the company or an individual staff member ever been refused, suspended or withdrawn/revoked within the last five years? | Yes, and further information is provided below.  Available on request: Click here to enter text.  No  Click here to enter text. |
| 13.2.3  N/A More | Does the company have a “living will”? *(Select all that apply)* | Attached/included: Click here to enter text.  Available for review onsite  Available on request: Click here to enter text.  Available online: Click here to enter text.  Not available for review  We do not have one  We are not required by law to have one |
| 13.2.4  N/A More | During the last five years (or the life of the company, if shorter), have all required tax returns been filed and taxes paid on time? | Yes  No, and details are provided below.  Click here to enter text. |
| 13.2.5  N/A More | What firm currently is appointed as auditor of the company’s financial statements? | Click here to enter text. |
| 13.2.6  N/A More | Have the company’s financial statements been qualified by its external auditor in the last 24 months? | Yes  No |
| 13.2.7  N/A More | Has the company or any affiliated entity ever failed to make payments under any secured or unsecured indebtedness? | Yes, and a description of each such situation is set out below.  No  Click here to enter text. |
| 13.2.8  N/A More | Has the company, an entity affiliated with the company or any current or former principal of the company ever filed for bankruptcy? | Yes, and a description of each such situation is set out below.  No  Click here to enter text. |
| 13.2.9  N/A More | (a) What types of insurance does the company have (other than cyber insurance discussed above)? *(Select all that apply)* | Professional indemnity  Errors and omissions  Social engineering  Building/contents (including IT hardware and office fixtures)  Other (Provide additional comments)  None of the above  Click here to enter text. |
| N/A More | (b) Has the company made an insurance claim on any of the above policies in the last 24 months? | Yes  No |
| 13.3 More Questions on Outsourcing by the Company to Third Parties | | |
| 13.3.1  N/A More | With respect to each of the **company’s** service providers (including, but not limited to, any affiliates and any providers of outsourced or delegated functions), provide following:  • name, address, LEI or register number (if any) and parent company (if any) of the provider;  • the service or outsourced function provided and the location(s) from which each such service or function will be provided;  • a brief description of the services provided;  • the appointment year;  • if a material outsource arrangement, the rationale for the outsourcing; and  •whether the service involves the third party having access to client data and, if so, where such data will be stored. | Attached/included: Click here to enter text.  Available on request: Click here to enter text.  We do not have any service providers or outsource/delegate any functions to other entities. |
| 13.3.2  N/A More | (a) How frequently does the company perform periodic reviews of quality of service, cost and additional value provided by its service providers listed in response to Question 13.3.1? | More frequently than quarterly  Quarterly  Semi-annually  Annually  Less frequently than annually  Never, and, as a consequence, (b)–(d) below have been left blank.  Never, and, as a consequence, the rows for Questions 13.3.2(b)-(d) in the template DDQ have been omitted. |
| N/A More | (b) Are the company’s reviews of service providers documented? | Yes  No |
| N/A More | (c) Does the company perform onsite reviews on all of its service providers? | Yes  Yes, but not all of them and the types included or excluded from such reviews are identified below.  No, and, as a consequence, (d) below has been left blank.  No, and, as a consequence, the row for Question 13.3.2(d) in the template DDQ has been omitted.  Click here to enter text. |
| N/A More | (d) How often does the company perform those onsite reviews? *(Select one)* | More frequently than quarterly  Quarterly  Semi-annually  Annually  Less frequently than annually |
| 13.3.3  N/A More | Have any company service providers, including, but not limited to the company’s auditors, been terminated or resigned within the last three years? | Yes, and details are provided below.  No  Click here to enter text. |
| 13.3.4  N/A More | Where outsourced providers and delegates are able to sub-outsource/sub-delegate, how does the company safeguard that the subordinated provider also complies with obligations applicable to the company towards clients and that any required examination and inspection rights are safeguarded? | Click here to enter text. |
| 13.4 Additional Questions | | |
| Further Question | Add a question below:  Click here to enter text. | Click here to enter text. |
| 13.5 Company Comments | | |
| Comment | Enter relevant question number:  Click here to enter text. | Click here to enter text. |

Explanations, Assumptions and Disclaimers

The space below has been provided for vendors to provide investment managers with any general explanations, assumptions and disclaimers that are relevant to the responses in this DDQ. If there are explanations or assumptions specific to individual questions, these should be included in the space provided for this purpose at the end of the applicable module with the relevant question(s) identified.

|  |
| --- |
| Click here to enter text. |

**This questionnaire was completed by (name):**

**The information in this questionnaire is accurate as of (date):**

By signing this questionnaire, you attest that the answers are complete and correct to the best of your knowledge and accurately reflect your company’s actual practices, policies, procedures and controls as of the date indicated above.

Date:

Signature:

Name:

Title:

Email:

Phone:



**Illustrative Questionnaire for the   
Due Diligence of   
Vendor Technology and Cyber Security**

# FURTHER INSTRUCTIONS

For members using this questionnaire to perform due diligence on vendors, it is important to remember that this questionnaire is simply a tool. Not all of the questions are going to be applicable to all vendors, but we recommend that members ask sufficient questions and request associated supporting material so that they are able to make an informed decision.

Members should review with their legal counsel and other advisors the value of the responses and to what extent, if any, they may rely upon such responses. The terms of any relationship with a vendor will normally be confined to the terms of the relevant contract. In order to obtain the best possible information on any specific vendor, additional questions should be raised to clarify any point of uncertainty and, where practicable, verbal examination should be undertaken.

While AITEC and AIMA have used all reasonable efforts to produce a questionnaire of general application in connection with a due diligence appraisal of vendors, prior to any member sending out the questionnaire, it is strongly recommended that the questions are reviewed and, where necessary, supplemented to suit its own requirements and its state of knowledge of the vendor’s operations.

Documents Requests; Attachments

Various questions in this DDQ request documents to be provided and often multiple options are given for how that information can be delivered. Some of these options require users to include certain additional information to help readers understand where/how they can access those materials:

* **Attached/included –** In the content control box following this option, the user should include the file name of the included or attached document where applicable and describe where and how the documents have been attached or included;
* **On request –** In the content control box following this option, the user should indicate where such requests should be sent and by what method; and
* **Online –** In the content control box following this option, the user should include the web address where the indicated material can be accessed.

Making Changes to the DDQ Template

It is strongly recommended that users neither alter nor delete any of the questions. The value of this questionnaire for members and vendors alike lies in the standardization of the questions to allow members to easily compare vendors and to reduce the workload of responding to different forms of questionnaire.

That said, if there are additional questions to be asked, there is a section at the end of each module set aside for this purpose and additions should not be made anywhere else. That space can also be used by an outsource provider to provide any clarifications or additional information not otherwise called for by the standard question set.

To signal to readers that there is something relevant to read in the additional questions section, users should tick the **“More”** option in the first column.

If a question is not applicable to the user’s business model, instead of leaving it completely blank or removing the row, consider simply ticking the **“N/A”** option in the first column to signal to readers that the question is not applicable. Although this option has been provided for each row, users should consider selecting the “Not applicable” option among the answer choices where such a choice is available rather than selecting the “N/A” option. Readers may follow up to ask further questions about why a company believes an individual question is not applicable.

**In the event of any questions being altered or omitted from this questionnaire, users are required to remove all references to AIMA from the document but may include the following statement in the header on each page: “This questionnaire is based on the AITEC-AIMA Illustrative Questionnaire for the Due Diligence of Vendor Technology and Cyber Security (2019).”**

The only exceptions to the general rule above are that:

* users presenting the DDQ in Word or PDF form may delete the rows containing the follow-on questions if they select the answer option in a question that signals to readers that template DDQ rows have been omitted; and
* users may omit the pages containing the “Further Instructions” and the attached “Terms of Use” when presenting the filled in DDQ to recipients; and
* if desired, users may remove any “N/A” and “More” options that are not ticked in the first column to make the ones that are ticked easier to identify.

Please answer all the questions. For many questions, there is a requirement to provide additional commentary depending on your answer to a yes/no question. Please include the additional information in the text box provided for such questions. For other questions, there is an option to provide additional text if you want to, but the text boxes for those questions can be left blank if a further explanation is not required.

To add questions, please use the “further questions” function at the end of the relevant section(s).

To add comments or further information in response to individual questions where no text box has been provided for that purpose, please use the “comments” function at the end of the relevant section(s).

Please do not delete or amend any of the content control boxes (except as discussed above) even though this is possible to do.

The content controls used in this document were not available for versions of Word up to and including Word 2010. They may also not be available in “mini” versions of Word available through Office 365, Google Docs, and various tablet apps. In these situations, the content controls may or may not be visible and/or operable. If you accidentally delete a content control, any response that would have been in the content control will no longer be tagged correctly for data extraction. As the document is in Word, it is possible to insert text outside the content controls, although this is not recommended and may adversely affect an outsource provider’s ability to make certain of the certifications. Any response outside a content control will not be tagged correctly for data extraction and will detract from the usefulness of the information for some users.

Material/Significant/Critical/Important Outsourcing to the Vendor

When regulated entities such as investment managers outsource functions to others, applicable regulations require enhanced due diligence on the vendor be performed, especially where the tasks, functions or services being outsourced to the vendor are “material”, “significant”, “critical” or “important” to the regulated entity’s provision of services to its clients. For information about when this might be the case and for a discussion of how these terms may be interpreted, please see AIMA’s Guide to Sound Practices for the Outsourcing by Investment Managers”.

Section 13 of this DDQ template has been prepared to provide a selection of the questions which are not covered elsewhere in the template but which may nevertheless be relevant when the relevant product/service would constitute a material/significant/critical/important outsourcing arrangement for the requesting investment manager. ***This section is OPTIONAL and may be removed by the requesting investment manager without affecting the ability to retain the template’s branding.***

Formatting

This DDQ has been formatted to fit on A4-sized paper. However, users that prefer Letter-sized paper can simply change the paper size. Please note that for best results this should be done on a section-by-section basis rather than simply changing it in a single place or changing it while having selected all.

Before finalizing your document, you should:

* delete this “Further Instructions” section and the “Terms of Use” section below, as well as the section break that separates these from the DDQ’s signature block;
* place your mouse anywhere in the table of contents, right click your mouse, select the “Update field” option and select “Update page numbers only” to update the table of contents; and
* update the page numbers shown in the “To the reader” note included at the top of each section of questions by right clicking on the page number shown (inside the grey shadowed box representing the field code) and selecting the “Update field” option to update the page number.



**Illustrative Questionnaire for the   
Due Diligence of   
Vendor Technology and Cyber Security**

# TERMS OF USE

The copyright in this questionnaire is the sole property of AITEC and AIMA.

The table below shows how this questionnaire is permitted to be used.

| **Action** | **Permitted Use/Not Permitted** |
| --- | --- |
| ***Circulation by AIMA manager members and AITEC members*** | |
| An AIMA manager member or AITEC member provides the blank DDQ to a vendor that is an AIMA member (or represented by an AITEC member) to complete | Permitted use |
| An AIMA manager member or AITEC member provides the blank DDQ to a vendor that is not an AIMA member (or represented by an AITEC member) to complete | Permitted use |
| ***Circulation by vendors that are AIMA members*** | |
| An employee of a vendor that is an AIMA member provides it to another employee of that vendor for its internal use | Permitted use |
| A vendor that is an AIMA member fills in DDQ and provides it to a requesting AITEC or AIMA member | Permitted use |
| A vendor that is an AIMA member fills in DDQ and provides it to a client/prospective client that is not an AIMA member | Permitted use |
| ***Circulation by investors that are AIMA members*** | |
| An investor that is an AIMA member (an ‘Authorised Investor’) provides the blank DDQ to a vendor that is an AIMA member to complete | Permitted use |
| An Authorised Investor provides the blank DDQ to a vendor that is not an AIMA member to complete | Permitted use |
| ***Use by vendors that are not AIMA members*** | |
| A vendor that is not an AIMA member obtains the blank DDQ from an Authorised Investor, an AIMA member or an AITEC member and fills it in and provides it only to requesting Authorised Investor, other requesting AIMA member or requesting AITEC member, as applicable | Permitted use |
| A vendor that is not an AIMA member obtains the blank DDQ (whether or not from an Authorised Investor, an AIMA member or an AITEC member) and fills it in and provides it to anyone other than an Authorised Investor, a requesting AIMA member or a requesting AITEC member | **Not permitted** |
| ***Circulation by other service providers that are AIMA members*** | |
| An employee of an AIMA service provider member provides it to another employee in the same office of that service provider member firm for its internal use | Permitted use |
| An employee of an AIMA service provider member provides it to another employee in a different office of that service provider member firm for its internal use | ***Permitted use if the receiving employee is in an office of the service provider that is itself an AIMA member; otherwise not permitted*** |
| An AIMA service provider member makes the blank DDQ available to a client that is an AIMA member | Permitted Use |
| An AIMA service provider member makes the blank DDQ available to a client that is not an AIMA member | **Not permitted** |
| ***Transformation to electronic form for onward circulation*** | |
| An AIMA member transforms the blank DDQ into an electronic format or other format to make available to its own clients that are AIMA or AITEC members | ***Permitted use only under the terms of a written licensing agreement with AIMA and AITEC*** |
| An AIMA member transforms the blank DDQ into an electronic format or other format to make available to its own clients that are not AIMA nor AITEC members | **Not permitted** |
| A non-AIMA member transforms the blank DDQ into an electronic format or other format to make available to its own clients that are AIMA or AITEC members | ***Permitted use only under the terms of a written licensing agreement with AIMA and AITEC*** |
| A non-AIMA member transforms the blank DDQ into an electronic format or other format to make available to its own clients that are not AIMA nor AITEC members | **Not permitted** |
| ***All other circulations and uses*** | |
| Any person provides a blank or completed DDQ to anyone except in the permitted use circumstances set out above | **Not permitted** |