

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

**(Short Form Version)**

|  |  |
| --- | --- |
| 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. |

[Short Form Questionnaire 2](#_Toc529872515)

[1. Company Information 2](#_Toc529872516)

[2. Product/Service Information 5](#_Toc529872517)

[3. Policies, Procedures, Standards and Controls 6](#_Toc529872518)

[4. Data Security 7](#_Toc529872519)

[5. System Maintenance 10](#_Toc529872520)

[6. Access Controls 11](#_Toc529872521)

[7. Infrastructure Security 13](#_Toc529872522)

[8. Physical Security 15](#_Toc529872523)

[9. Business Continuity 16](#_Toc529872524)

[10. Cyber Incident Response 18](#_Toc529872525)

[11. Software Development 18](#_Toc529872526)

[12. Additional Questions 19](#_Toc529872527)

[13 Company Comments 19](#_Toc529872528)

[FURTHER INSTRUCTIONS 20](#_Toc529872529)

[TERMS OF USE 22](#_Toc529872530)

| Short Form Questionnaire | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *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 starting on page 19. | | | | | | | | |
| 1. Company Information | | | | | | | | |
| 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. | | |
| 1.3 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. | | | |
| 2. Product/Service Information | | | | | | | | |
| 2.1  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. | | | |
| 2.2  N/A More | Please describe the nature of the relevant product and/or service. | | | | Click here to enter text. | | | |
| 2.3  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. | | | |
| 2.4  N/A More | Does the company have any dedicated cyber security staff supporting the relevant product and/or service? | | | | Yes  No | | | |
| 3. Policies, Procedures, Standards and Controls | | | | | | | | |
| 3.1  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. | | | |
| 3.2  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. | | |
| 3.3  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. | | |
| 3.4  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  Not applicable  Click here to enter text. | | | |
| 3.5  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. | | | |
| 3.6  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. | | | |
| 4. Data Security | | | | | | | | |
| 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. | | | |
| 4.2 Mobile Access | | | | | | | | |
| 4.2.1  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) below has been left blank.  No, and, as a consequence, the row for Question 4.2.1(b) in the template DDQ has 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. | | | |
| 4.2.2  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) below has been left blank.  No, and, as a consequence, the row for Question 4.2.2(b) in the template DDQ has been omitted.  Click here to enter text. | | | |
| N/A More | (b) 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. | | | |
| 4.2.3  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) below has been left blank.  No, and, as a consequence, the row for Question 4.2.3(b) in the template DDQ has 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. | | | |
| 4.2.4  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) below has been left blank.  No, and, as a consequence, the row for Question 4.2.4(b) in the template DDQ has 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. | | | |
| 4.3 Data Loss Prevention | | | | | | | | |
| 4.3.1  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. | | | |
| 4.3.2  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. | | | |
| 4.3.3  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. | | | |
| 5. System Maintenance | | | | | | | | |
| 5.1  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  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(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(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. | | | |
| 5.3  N/A More | 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  Click here to enter text. | | | |
| 6. Access Controls | | | | | | | | |
| 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. | | | |
| 6.2 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)-(g) below have been left blank.  No, and, as a consequence, the rows for Questions 6.2.1(b)-(g) 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) 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 | (f) 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 | (g) Does the company’s system provide access audit reports for client review? | | | | 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 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 | | | |
| 7. Infrastructure Security | | | | | | | | |
| 7.1  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. | | |
| 7.2  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) below has been left blank.  No logging of this activity, and, as a consequence, the row for Question 7.2(b) in the template DDQ has been omitted. | | | |
| N/A More | (b) 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. | | | |
| 7.3  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 | | | |
| 7.4  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 7.4(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. | | | |
| 7.5  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. | | | |
| 7.6  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 7.6(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 7.6(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. | | | |
| 8. Physical Security | | | | | | | | |
| 8.1  N/A More | 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.  Click here to enter text. | | | |
| 8.2  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 8.2(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. | | | |
| 8.3  N/A More | 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).  Click here to enter text. | | | |
| 9. Business Continuity | | | | | | | | |
| 9.1 Policy | | | | | | | | |
| 9.1.1  N/A More | Has the company developed a Business Continuity Plan (BCP)? | | | | 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 | 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. | | | |
| 9.2.2  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 9.2.2(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. | | | |
| 9.2.3  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. | | | |
| 9.2.4  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. | | | |
| 9.2.5  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. | | | |
| 9.2.6  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. | | | |
| 10. Cyber Incident Response | | | | | | | | |
| 10.1 Detection and Response | | | | | | | | |
| 10.1.1  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. | | | |
| 10.1.2  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 Cyber Incidents | | | | | | | | |
| 10.2.1  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 10.2.1(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. | | | |
| 10.2.2  N/A More | Has the company ever made a claim on a cybersecurity insurance policy? | | | | Yes, and details are provided below.  No  Click here to enter text. | | | |
| 11. Software Development | | | | | | | | |
| 11.1  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 11.1.2-11.1.3 in the template DDQ have been omitted. | | | |
| 11.2  N/A More | Are separate environments maintained for development, testing and production? | | | | Yes  No, and details are provided below.  Click here to enter text. | | | |
| 11.3  N/A More | Does the company prevent client data from being used in non-production environments and systems unless obfuscated or scrambled? | | | | Yes  No | | | |
| 12. Additional Questions | | | | | | | | |
| Further Question | Add a question below:  Click here to enter text. | | | | Click here to enter text. | | | |
| 13 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**

**(Short Form)**

# FURTHER INSTRUCTIONS

**This form of the questions related to the diligence of vendor technology and cyber security represents a condensed version of the AITEC-AIMA Illustrative Questionnaire for the Due Diligence of Vendor Technology and Cyber Security (2019). Members using this questionnaire should consider whether and to what extent they need or want more information than has been provided in this short form version.**

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.

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 (Short Form) (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.

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 number shown in the “To the reader” note included at the top of the first 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**

**(Short Form)**

# 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** |