Sample Preliminary Due Diligence Questionnaire (DDQ)

By: Catherine Tibaaga

Listed below is a set of questions that a due diligence questionnaire (DDQ) should capture. The questions should be sent to the third-party to determine potential residual risks prior to undergoing a full third-party risk assessment. The list does not represent the full set of potential questions. They represent a sample list that can be expanded. ***Please ensure that a Non-Disclosure Agreement (NDA) is executed prior to sending the DDQ out to the third-party.***

1. **Third-Party Contact Information:** Vendor Name, Address, Point-of-Contact Name, Phone Number and Email

2. **Description of Services/Products:** What services/products will your organization provide to the client?

3. **Cost:** How much will the services/products cost? *Please attach a quote*.

4. **Office Locations:** How many office locations does your organization have? *Please include the locations of your organization.*

5. **Data Center Locations:** How many data centers does your organization utilize to provide services/products to the client? *Please include the locations of the data centers utilized by your organization.*

6. **Business Entity:** What is your business entity type?
**Example: Sole Proprietorship, Partnership, C Corporation, S Corporation, Limited Liability Corporation (LLC), Limited Liability Partnership (LLP)*

7. How many employees and contingent workers do you have in your organization? Use a scale.
**Example: 1-10, 10-50, 50-100, 100-500, 500-1000, 1000 or more*

8. **Physical Access:** Does your organization need to be onsite or offsite to provide services/products to the client?

9. **System and Equipment Access:** Will your organization use your own systems and equipment to perform the services or will your organization need access to the client's systems, equipment and network?

10. **Description of Data:** What data is needed to provide the services/products to the client?
**Example: Name, Social Security Number, Trade Information, Source Code*

11. **Access to Data:** How is your organization accessing client data?
**Example: Is the data supposed to be sent to your organization via email or will the data need to be uploaded to an application?*

**Note: For third-parties that are providing an application to perform the services, please specify whether the application will be an internally hosted solution, cloud-based solution (i.e. SaaS, IaaS, PaaS), or a traditional web-based application (i.e. eBay, WebEx, online banking application)*

12. **Data Storage:** Does your organization outsource data storage or does your organization utilize its own databases to store data?

13. **Segregation of Data:** Does your organization's database structure allow segregation of sensitive client data?

14. **Independent Attestations:** Does your organization have independent attestations such as (i.e. ISO 27001, SSAE-18, PCI- DSS, ISO 9001)?

<u>Preliminary Risk Questionnaire</u>
For all questions, please provide a response. If it is not applicable, please provide a response of N/A.

- **Information Security**
    - Does your organization have documented information security policies and procedures?
    - How often are the information security policies and procedures reviewed and updated?
    - Who in the organization is responsible for reviewing and updating the information security policies and procedures?
    - Does your organization have privacy policies and procedures?
    - How often are the privacy policies and procedures updated?
    - Who in the organization is responsible for reviewing and updating the privacy policies and procedures?
    - What methods of encryption are utilized for data at rest and in transit?
    - Are the encryption methods utilized FIPS 140-2 approved?
    - Does your organization utilize firewalls to filter incoming data and information from the internet into your company network?

- Does your organization perform penetration testing at least once per year to determine if unauthorized access to the computer network and malicious activity is possible?

- Does your organization perform vulnerability testing at least once per year in order to identify vulnerabilities within the network?

- Does your organization perform background checks on employees and contingent workers prior to onboarding them?

- Does your organization utilize multi-factor authentication?

- Does your organization utilize scan cards or biometric scans to grant employees and contingent workers access to the building and data centers where data is stored?

- If offering a technology product, does the organization utilize software development life cycle (SDLC) or Agile to build and maintain technological product?

- Does the technological product undergo information security testing and quality assurance testing prior to deployment?

Risk Management

- Does your organization have an enterprise risk management framework implemented at your organization?

- Does your organization have documented enterprise risk management policies and procedures?

- Who in the organization is responsible for reviewing the enterprise risk management policies and procedures?

- Does your organization utilize an outside third-party to provide services/products to the client?

- Does your organization have a third-party risk management program (TPRM)?

- Does your organization include right-to audit clauses in contracts with third-parties?

- Does your organization have a certificate of insurance (COI)? *Please attach a copy of your COI.*

Business Continuity/Disaster Recovery

- Does your organization have a business continuity plan?

- How often is the business continuity plan updated?

- Does your organization conduct business continuity tests once per year?
- Does your organization have a disaster recovery plan?
- How often is the disaster recovery plan updated?
- Does your organization conduct disaster recovery tests once per year?
- Does your organization have business continuity and/or disaster recovery sites?
- Are the business continuity/disaster recovery sites located in the United States or outside the United States? *Please include the locations of business continuity/disaster recovery sites?*

**Note: Questions can be utilized to determine if outsourcing to a third-party is within the risk appetite for third-party risk management. To determine if a third-party fits within the TPRM risk appetite, TPRM should utilize the questions in the preliminary DDQ and assign each question a weighted score.*

- *TPRM should work with the risk SMEs for each risk area to assign the correct score to each question.*
- *Each question in the preliminary DDQ reflects corporate, industry and regulatory standards for each risk area (i.e. information security, business continuity, disaster recovery, financial, compliance, and reputational).*
- *To produce a preliminary residual risk score, the third-party should complete the preliminary DDQ and the preliminary DDQ should assign a score based on the responses provided by the third-party.*
- *The preliminary residual risk score should be based on a preliminary residual risk scoring scheme that is determined and approved by TPRM, the risk SMEs, ERM/ORM. It should be automated within the preliminary DDQ.*
- *The preliminary residual risk scoring scheme represents the third-party risk appetite for the organization. Please refer to the example below.*

Residual Risk Score	Residual Risk Classification	Inside or Outside TPRM Risk Appetite	Action Required
25-30	Very Low	Inside	Move forward with TPRM process.
21-25	Low	Inside	Move forward with TPRM process.
16-20	Medium	Inside	Move forward with TPRM process.

6-15	High	Outside	Find an alternative third-party or ask for independent attestation. If independent attestation exists, move forward with TPRM process.
0-5	Very High	Outside	Do not utilize third-party. Find an alternative third-party.

- *All residual risk scores should be recorded in the residual risk register. When performing data analytics, TPRM should determine the percentage of third-parties within the third-party population that fit within the defined third-party risk appetite as defined by the residual risk scoring scheme utilized in the preliminary DDQ.*