Inherent Risk Identification Tool Questionnaire

Listed below is a set of questions that a risk identification tool should capture. The questions should enable the organization to understand the risks inherent to the products and/or services that the vendor will provide. The list does not represent the full set of potential questions. They represent a sample list that can be expanded.

1. **Vendor (s) Information:** Vendor Name, Address, Point-of-Contact Name, Phone Number and Email

**Note: If there is more than one vendor that is being considered under a Request-For-Proposal (RFP), then the tool should allow whoever in the organization is responsible for managing the day-to-day relationship to capture the various vendors being considered.*

2. **Description of products/services:** What products/services will the vendor be providing to the organization?

3. **Cost:** How much will the services cost the organization?

4. **The Service Type Classification:** our procurement function should have a list of service type classifications that correspond to the various products/services provided to your firm.

5. **Physical Access:** Will the vendor provide the products/services onsite or offsite?

6. **System and Equipment Access:** Will the vendor use their own systems and equipment to perform the service or do they need access to the organization?

**Note: For firms that hire consulting firms such as the Big Four, many of the organizations may need to utilize your organizational resources (i.e.Laptops, network access) in order to provide the services.*

7. **Description of Data:** What is the data that is being sent to the vendor?

**Example: Name, Social Security Number, Trade Information, Source Code*

8. **Data Classification(s):** What is the data classification of the data being provided to the vendor?

*Example:

Data Classification	Description
Very Confidential	Highly sensitive company confidential information (i.e. source code, trade information, financial models, etc).
Confidential	Information that cannot be found in the public domain such as company confidential information.
Public	Information that could be found in the public domain (i.e. internet, news sources, etc).
Personal Identifiable Information (PII) or Public Health Information (PHI)	*NIST 800-122 Definition of PII:* Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. For the definition of PHI, please refer to the link for HIPAA.

**Note: If more than one data classification is involved, then choose the highest data classification. For example, if the data being sent to the vendor includes confidential information and PII, then the vendor should choose both public and PII.*

9. **Access to Data:** How is the data is being accessed by the vendor?

**Example: Is the data being sent to the vendor via email or will the data be uploaded to the vendor's application being provided by the vendor.*

**Note: For vendors that are providing an application to perform the services, it is essential that the risk identification tool capture whether the tool will be an onsite premise solution, cloud-based solution (i.e. SaaS, IaaS, PaaS), or a traditional web-based application (i.e. eBay, WebEx, online banking application) as this tool will be used as a platform to access the data.*

10. **Vendor’s Recovery Time Objective (RTO):** What is the vendor’s recovery time in the event they experience a business disruption (i.e. 24, 48, 72 or more hours)?

11. **Regulatory Impact:** Are the products/services being provided impacting financial reporting or any regulatory/compliance reporting (i.e. SOX, SEC filings)?

12. **Other:** Any other pertinent information that describes the nature of the engagement.