

e. What countries do you operate in?

f. How many years have you been in business?

g. Do you plan to utilize other companies in the proposed engagement, including subsidiaries, affiliates, partnerships or joint ventures, or individuals other than your own employees to operate under the proposed agreement?

YES NO

i. If yes, identify the name and address of the company or individual you will use, explain your relationship with them and the actions they will implement.

Name/Address	Relationship	Activities

h. Do you have a code of ethics and/or anti-corruption code? If so please provide on a separate page.

YES NO

i. Identify your compliance officer, if applicable.

2. Ownership and Key Employees

a. List the name and title of the owners of your company.

Name	Title

i. Indicate if any of these individuals have an ownership stake in your company.

b. List your company's key officers and members of the Board of Directors.

Name	Title

c. List your company's employees and managers who will be primarily responsible for performing and supervising services under the proposed agreement.

3. Risk Management

- a. Have you conducted a risk assessment in the past year and do you have a risk management policy in place?

YES NO

- b. Are there physical controls, surveillance and monitoring to detect unauthorized access?

YES NO

- c. Do you conduct regular security awareness training for your employees?

YES NO

- d. Describe your company's business insurance. Are you insured for general liability, cybersecurity and professional indemnity (e.g., E&O and D&O insurance)?

- e. Do you have a business continuity plan or disaster recovery plan, and are all response procedures tested regularly?

YES NO

- f. Is there a protocol for notifying key stakeholders and customers in the event of a data breach or other security incident? If yes, how quickly after the breach are stakeholders and customers notified?

YES NO

4. Cybersecurity Risks

- a. Do you have official cybersecurity policies and procedures in place?

YES NO

b. Do you have processes for risk mitigation and remediation?

YES NO

5. Network, Application, and Information Security

a. Do you have real-time networking monitoring to identify unauthorized access and breaches?

YES NO

6. Compliance

a. Data Protection and Privacy

i. What data do you gather and save? How is that data utilized?

ii. Who has authorization to access third-party data?

iii. How is confidential data maintained? Who is responsible for maintaining and destroying confidential data?

iv. Provide your company's privacy policy on a separate page.