Information/Cyber Security Due Diligence – Frequently Asked Questions for Suppliers

	Question	Answer
1.	Why do I have to complete an Information/cyber security survey?	LSEG's Third Parties are required to support the onboarding process by completing a cyber security assessment. The type of cyber assessment is triggered based on the level of risk and criticality associated with the services provided by the Third Party.
2.	What language can the answer and evidence documentation to be provided in?	English. The official language of the firm is English. Third Parties with documents in other languages are required to provide translated copies to us.
3.	How does the Due Diligence process work?	The Due Diligence process is managed by the Third-Party Assurance team, who will engage the Third Party initially. If a cyber assessment is required (based on the risk level of the services) the vendor will receive an email from Prevalent. Cyber assessment and review of the surveys and Third-Party documentation is managed by the LSEG Cyber Security Third Party Assurance team.
4.	How long will the Third Party have to complete the Cyber Questionnaire?	15 working days
5.	Does the Third Party have to provide evidence documentation?	Yes
6.	What type of evidence documentation will LSEG accept from Third Parties?	Each question will have a desired Information Security documentation listed. We also accept SOC 2 reports, HITRUST type documents, ISO Certification and Statement of Applicability. Please note we may contact Third Parties if we identify gaps in the documentation provided.
7.	What happens after the Third Party completes the Cyber Survey?	The LSEG Cyber team will review the submission, if there are any gaps in control or evidence documentation, the team will contact the Third Party to resolve these gaps.
8.	Does the Third Party have to complete Due Diligence again?	Yes. Annually or every few years based on the risk associated with the services. This is to ensure compliance with regulatory and policy requirements.
9.	Do Third Parties have to provide answers at an enterprise level?	Yes. LSEG completes cyber assessments on its vendors at an enterprise level to understand their security posture, not solely on the services being provided.