**Project Genesis**

**Scope of Work: Technology Due Diligence (red flag assessment)**

We will perform a Technology Due Diligence (“Tech DD”) on the Target entity and provide a red flag report on the material risk items pertinent to the proposed transaction.

We have structured our proposed scope of work based on your requested areas for review but with a specific focus on the IT applications and underlying infrastructure.

|  |  |  |  |
| --- | --- | --- | --- |
| **Scope Area** | **Scope Focus** | **Full/Limited** | **Hours** |
| **Phase 1** | | | |
| **IT Applications** | * Assess the application landscape (including an understanding of peripheral/support systems vs core systems used in the running of operations). * Assess the applications’ fit for current and future business growth requirements. * Assess self-developed applications vs off-the-shelf applications (including an understanding of licencing agreements). * Assess application integration to support data flow and reporting. * Assess the scalability of the application layer to support the expansion and diversification of the target’s current product offering. * Assess the product and innovation roadmap for the technology landscape. * Assess the Operational Tech landscape (DCS/SCADA/MES systems) in accordance with above criteria as applicable. | Full | **16**  **(3hrs OT)** |
| **IT Infrastructure** | * Assess the IT infrastructure environment and respective operations. * Assess the infrastructure’s fit for current and future business growth requirements in the following areas: Data centre and hosting, end user computing, and networks. * Assess the backup procedures, disaster recovery plans and business continuity plans, including any performed tests and results. * Overview of past IT outages/disruptions and the mitigations undertaken, including an assessment of known IT gaps. * Assess the scalability of the IT infrastructure to support the expansion and diversification of the target’s current product offering. * Assess the Operational Tech infrastructure environment (PLC/Networks/Redundancy of Power and Networks) in accordance with above criteria as applicable. | Full | **16**  **(3 hrs OT)** |

**Exclusions:**

* In-depth assessment of technical debt (application code/configuration reviews and application technical designs reviews)
* Detailed platform architectural reviews
* Detailed audit of relevant staff skills
* Detailed analysis of IT security audit  (internal/external)
* Detailed specialist cyber and security audit or performing specialist procedures (i.e., penetration testing, vulnerability testing)
* Detailed governance maturity assessment audit
* Detailed IT control design and implementation assessment for user access management, program change management, IT governance and incidents and problem management.