**thScope**

**Definitions**

**Full scope**: defined as an in-depth analysis of the relevant IT scope area with an output report including a detailed executive report and selected information.

**Limited scope**: defined as a high-level assessment focused on aspects of the IT scope that are fundamental to the business. This would result in key findings consideration, and where applicable an executive report.

**Deliverables**: IT due diligence report

* IT overview (At-a-Glance)
* IT key findings & considerations
* IT executive report
* Selected information

|  |  |  |  |
| --- | --- | --- | --- |
| **Scope Area** | **Scope Focus** | **Scope** | **Expected hours** |
| **IT governance** | * Overview of the IT governance and oversight arrangements. * Review the IT governance framework and processes, including an overview of the main IT policies, standards, and procedures (e.g., problem and incident management, program change management, disaster recovery, etc.). * Assess the IT risk management processes. * Assess IT compliance management and regulatory requirements. * Understand the key elements of the software development process. | Limited scope |  |
| **IT strategy** | * Understand key historical IT milestones and current IT strategy and roadmap for IT.​ * Understand the current IT strategy and general strategic IT principles (e.g., use and adoption of cloud infrastructure). * Understand the IT roadmap and current major initiatives. * Understand the digital strategy. (i.e., assess current initiatives towards the digitization of internal processes, digital services, and new digital products). | Limited scope |  |
| **IT applications** | * Overview of key business applications. * Use of open systems, commercial off the shelf (COTS) applications. * Assess application landscape and fit for current and future business requirements.​ * Assess custom applications and automation gaps. * Assess application integration to support processing, data flow and reporting. | Full scope |  |
| **IT infrastructure** | * Assess IT infrastructure environment and respective operations and fit for current and future business requirements in the areas data center and hosting, cloud, end user computing, networks and telephony​. * Analysis of backup procedure and disaster recovery plans incl. performed tests. | Full scope |  |
| **IT organisation** | * Analyse the IT organization in terms of size and skills as well as potential external dependencies (key person dependency risk). * Analysis of the IT operating model in terms of key capabilities. * Use of external service providers and contractors. | Full scope |  |
| **IT financials & contracts** | * Assess historical and planned IT spend (capex and opex) incl. breakdown. * Evaluate IT spend based on Industry benchmarks​. * Evaluate degree of outsourcing and key IT suppliers​. * Assess management o of IT suppliers and service levels. | Limited scope |  |
| **IT projects** | * Analyse IT Project Portfolio and alignment with business strategy​. * Understand the focus of IT projects (innovation vs. IT renewal)​.Assess critical / large projects (e.g., ERP implementation). | Limited scope |  |
| **IT security** | * Review current technical and organizational measures for cyber security and data privacy.​ * Analysis of any internal / external performed IT audits and penetration tests and respective results and mitigations undertaken. * Assess cyber and information security, and data privacy policies and procedures in place (including policies for data retention, data disposal, vulnerability and patch management, user access management, etc.). | Full scope |  |
| **Digitisation capabilities** | * Assess current initiatives towards digitization of internal processes, digital services and new digital products. * Evaluate current digital capabilities to support digital journey of the company. | Limited scope |  |

**Exclusions**

* Review of cybersecurity policies and procedures does not include a controls review.
* Review of infrastructure configurations.
* Other than a review of the internal/external audit reports, no review of controls will be performed.
* In-depth assessment of technical debt (application code reviews and application technical designs reviews).
* Detailed platform architectural reviews.
* Detailed audit of relevant staff skills.
* Detailed analysis of IT security audits.
* 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.

**Optional services (separate scoping & pricing)**

* If any material cyber findings are found, and further analyses requested, this will be subject to additional scoping & pricing.
* Should integration services become a priority for the transaction, and additional services requested in this regard, this will be subject to additional scoping & pricing.