

**Supplier Self Assessment**

**Cyber Security**

**Approved by TaylorWessing**

**Overview** > this assessment focuses on cyber security, asking suppliers to provide evidence and information on policies, procedures and system implementations in place to protect them and their customers / suppliers from cyber attacks or data breaches. The questions in this assessment are broadly formed to allow for easier completion of the questionnaire and emphasize a supplier’s focus on cybersecurity practices.

**Supplier target** > any supplier that deals with sensitive data and uses information systems in their business practice

**Scoring** > this assessment is scored based on the answers given. The recommended perspective for viewing the score is **Disruption Risks**

**🚩 Red flag questions** > there are no red flag questions in this assessment

**FAQ**

**NIS2 Directive & Digital Operational Resilience Act (DORA)**

The NIS2 Directive establishes a unified legal framework to uphold cybersecurity in 18 critical sectors across the EU.

The Digital Operational Resilience Act (DORA) applies to financial entities as outlined in Art. 2 para. 1 DORA.

Both frameworks have been taken into account in this questionnaire, without being specifically named. Relevant points from these regulations have been summarised and added in several of the questions in this Assessment

**Penetration testing**

The importance and prevalence of pentesting has been addressed in this questionnaire, aiming to check whether suppliers conduct such testing to identify possible security vulnerabilities.

**Company size and exemptions**

To provide a straightforward and broad questionnaire under cyber security practices, we have not included any segmentation based on regulation in relation to company size. The segmenting in business sizes as well as in entities would mean that, on the one hand, suppliers would have to carry out a legal review to determine whether they are subject to the DORA or the NIS2 Directive, and on the other hand, that some suppliers would have few or no cybersecurity obligations. This questionnaire is thus aimed at suppliers who do indeed have cyber security obligations.