Overview Risk Assessments

Rabobank overview of risk assessments for suppliers

Rabobank

Growing a better world together.

Risk Assessments

Important objectives of Rabobank's procurement activities are to mitigate risks regarding suppliers and to comply with laws and regulations. To achieve these objectives Rabobank assesses the following risks relating to suppliers and to contracts before entering a relationship with a supplier:

1. **Tier classification**
   Requirement: Contracts are categorized based on their inherent risk level. The higher the inherent risk level, the more effort is required for supplier due diligence and contract risk assessments. All contracts must have a tier classification to determine which risk assessments must be performed on the contract and when the reassessment of the contract must take place.
   Explanation: The inherent risk level of the product/service determines the required steps to be taken during the initial risk assessment and during the lifecycle management of the contracts to be in control of the supplier and contract and have an acceptable level of residual risk. Inherent risks are categorized into 5 tiers of criticality, ranging from critical inherent risk (tier 1) to low inherent risk (tier 4) for the bank. Tier 5 applies to products and services where no written contract with the supplier is required. All contracts for critical or important outsourcing arrangements and all contracts for which the AIC (Availability, Integrity, Confidentiality) score has an Availability and/or Integrity score of 3 fall into the tier 1 category.

2. **Outsourcing**
   Requirement: Contracts that qualify as cloud or non-cloud outsourcing according to the definition of applicable laws and regulations , follow the outsourcing process.
   Explanation: Outsourcing of activities Rabobank would normally do itself, to third parties or other Rabobank entities, requires extra attention. Requirements for outsourcing arrangements are explained in different laws and regulations. We follow extensive risk assessments and register outsourcing activities.

3. **Financial due diligence**
   Requirement: The financial stability of the supplier will be assessed.
   Explanation: Financial stability of a supplier is important for the continuity of the supply of goods and services and/or the relationship with the supplier.

4. **Sanctions**
   Requirement: All (potential) suppliers have to be checked against sanction and exclusion lists based on geographic or company related elements. A match with one of these lists results in a ban to do business with such a supplier.
   Explanation: Exclusion listings can be both internal and/or external and results in

suppliers with whom we are not allowed to do business with.

5. **Corruption**
   Requirement: Suppliers need to be screened on corruption indicators in accordance with applicable laws and regulations.
   Explanation: Rabobank has zero tolerance towards and is fighting corruption, as part of its mission 'Growing a better world together'. Corruption constitutes a serious integrity risk for Rabobank and its reputation. In addition to integrity and reputation risk, legal, regulatory or financial risks or consequences may arise for Rabobank from violation of corruption related laws and regulations.

6. **Conflicts of interest**
   Requirement: It will be assessed whether a conflict of interest could arise by entering into or maintaining a relationship with a supplier. Appropriate measures have to be taken if a conflict of interest can exist.
   Explanation: Internal policies on conflicts of interest provide minimum requirements for identifying, assessing, mitigating, preventing, managing and registering conflicts of interest.

7. **Privacy**
   Requirement: All (potential) suppliers have to be checked to see if their Processing of Personal Data complies with the EU General Data Protection Regulation (GDPR) and the ruling on the Schrems II verdict. Furthermore, suppliers must comply, if applicable, to local privacy regulations.
   Explanation: Rabobank cannot do business with suppliers who cannot guarantee the correct protection of private data as Rabobank remains accountable when our suppliers process personal information on Rabobank's behalf.

8. **Recovery and resolution**
   Requirement: Contracts with suppliers that qualify as resolution relevant have to be resolution resilient, which means they include specific legal clauses. Specific data of these contracts are registered in Rabobank's contract database.
   Explanation: Because of the vital functions of banks in society, banks need to prepare for a situation that they are failing or likely to fail. In order to achieve this, the EU has published the Bank Recovery and Resolution Directive which is implemented in national law.

9. **Business continuity**
   Requirement: Every supplier that contributes to the operational processes of Rabobank needs to provide assurance on the business continuity measures taken, in line with the Rabobank requirements on Business Continuity.
   Explanation: The continuity of critical services of Rabobank depends on the continuity of suppliers that contribute to that service. Critical suppliers and, suppliers of critical or important outsourcing, need to implement continuity measures that fit within the continuity objectives of Rabobank.

10. **Information security**
    Requirement: A security assessment needs to be performed on every contract.
    Explanation: As a bank we have to be permanently aware of the trust that is placed

in us by our clients, employees, suppliers and society as a whole. As Rabobank we have to ensure that the security risks are adequately managed by our suppliers. We have to be diligent with regard to protecting our core systems, communication channels and data. Our (information) technology landscape is becoming increasingly open by using cloud services and by connecting to other (mobile) networks. Security is now more important than ever, and we are responsible to be on top of developments in this domain in order to fulfil our role as a trusted bank within society.

11. **Subcontractors**
Requirement: An actual overview of material subcontractors is needed for each contract. Subcontractors need to undergo a risk assessment, to ensure that Rabobank is in control of the whole supply chain.
Explanation: Subcontractors need to be checked to ensure these subcontractors can deliver their products and services to Rabobank's suppliers in line with the required risk and compliance requirements for these suppliers. If a supplier uses subcontractors which are not able to comply with these requirements it can be reason for not signing or ending a contract.

12. **Exit plan**
Requirement: Rabobank has an exit plan in place for contracts in tier 1 and all critical or important outsourcing. For other tiers this is optional. Exit plans are tested every year.
Explanation: The exit plan is intended to ensure the orderly cessation of services by the supplier, regardless of intent or cause.

13. **Service level agreement**
Requirement: The performance of a supplier is actively monitored based on the service levels agreed. If service levels are not met, appropriate corrective actions need to be taken.
Explanation: To assure the service levels (such as delivery time, support or availability) between Rabobank and supplier, each contract concerning the delivery of services to Rabobank in tier 1, 2 and 3 has a Service Level Agreement. This is optional for tier 4 contracts.

14. **Outsourced staff**
Requirement: Outsourced staff is third party staff that is selected by the supplier to perform the agreed services. In case of outsourced staff, the supplier is responsible for their behavior, the adequate skills and knowledge, also on (compliance) risks and preventing conflicts of interests. When outsourced staff have access to Rabobank systems or locations, they need to undergo a security screening.
Explanation: Outsourced staff are not employees of Rabobank but are third party staff who are not selected by Rabobank but by the supplier. Outsourced staff work under their employer's (or contractor) supervision, e.g. the supplier.