NOVARTIS | Reimagining Medicine

Third Party Risk Management Guideline

Novartis Global Guideline

Effective: October 1st, 2020
Version ERC.303.EN.V1

Ethics Risk & Compliance
Third Party Risk Management

Contents

1 Introduction

1.1 Purpose

The Novartis purpose is to reimagine medicine to improve and extend people's lives. This requires the management of risks to maintain them at an acceptable level.

This guideline aims to assist Novartis in managing risks associated with Third Parties by:

- Defining the fundamental principles governing the management of Third Party risk at Novartis
- Clarifying Novartis expectations of associates on what they must know and adhere to before making any commitments with Third Parties
- Establishing roles and responsibilities of the key stakeholders involved in the management of Third Party risks

Adherence to this guideline will ensure that Third Party risks are managed in a holistic and consistent manner that enhances our capability to build and protect value for our stakeholders and patients, and advances the broader interests of society as a whole.

1.2 Scope and applicability

This guideline applies to all Novartis associates (hereinafter referred to as "associates"). Third Party types and risks managed within the scope of the TPRM Framework can be found here. Further information is available at the following link: FAQ

1.3 Key stakeholders in the management of Third Party Risks

The Novartis Third Party Risk Management (TPRM) framework is designed to manage interactions with Third Parties for the purpose of assessing, mitigating and monitoring the ongoing risk that each Third Party relationship represents.

The key stakeholders of this framework are:

- The Business Owner, who is the associate who holds the relationship with the Third Party and who therefore ultimately owns the risk
- The Risk Functions, which define specific risk policies in their area of responsibility
- The TPRM function, which maintains the TPRM framework and oversees the global operating model

Additional stakeholders include:

- The Procurement function, which partners with the Business Owner to ensure that the source-to-contract process complies with the requirements of this guideline
- The ERC TPRM champions, who act as an interface between the local stakeholder groups and the TPRM function

The detailed roles and responsibilities of each stakeholder group are defined in Section 3.

2 Principles

TPRM is built on five overarching principles

1. Maintain risks at an acceptable level

Novartis works with Third Parties who conduct business in a manner that is consistent with our values and standards, as defined in the Novartis Third Party Code.

A robust and risk-based assessment process is in place to ensure that Third Parties operate to the same standards as our own.

In this way, Novartis maintains risks at an acceptable level for both our organization and society at large.

2. Business owns the risk

The Business Owner owns and manages the risks identified with the Third Party during the entire Third Party relationship lifecycle.

The Risk Functions and the TPRM Function support the Business Owner in this task, namely to identify, assess, remediate (where applicable) and monitor risks. The Procurement function provides additional support within its role in managing the source-to-contract process.

3. Use the TPRM process

The TPRM Framework enables Third Party risk assessments to be managed through a risk-based approach in a single, mandatory process and system. The framework is scalable and flexible to enable the inclusion of additional risks over time.

The Business Owner initiates the Third Party risk assessment process. The outcome of the risk assessment determines whether a commitment with the Third Party can be made or if additional steps (e.g. remediation) are first required.

4. No Assessment, no contract

No transaction with the Third Party can be made before the risk assessment has been completed.

Where so-called “No-Go” criteria are identified during the risk assessment, no collaboration with the Third Party is possible.

5. Remain vigilant

Third Parties are monitored on an ongoing basis throughout the entire lifecycle relationship. This may include Third Party audits and subsequent remediation actions (where required) as defined by the relevant Risk Function.

Effective monitoring also requires the Business Owner to share with the stakeholders any relevant information that they become aware of which may have an impact on the risk classification of the Third Party.

A re-assessment of the Third Party is triggered every three years at the latest - or earlier in certain circumstances (e.g., where the contract is extended or renewed or the nature of our relationship with the Third Party changes significantly).

3 Roles and responsibilities

Business Owner	• Own the Third Party Risk, including ultimately deciding together with the Risk Functions whether to accept risks identified through the TPRM process • Carry out all Business Owner tasks as defined, such as: - Initiate the risk assessment process - Provide accurate and complete data on request and support requests for information or queries from the Risk Functions - Review and follow up on the Risk Function recommendations subsequent to the Third Party risk assessment - Drive any required remediation activities to address identified risks from prospective Third Party engagement - Liaise with Legal to ensure that any specific contract clauses required as a result of the risk assessment and the risk exposure are included in the contract with the Third Party
Risk Functions	• Define the specific Risk Function policy landscape (i.e. risk definition, risk position, risk indicators, assessment process steps, no-go criteria and escalation process) • Liaise with Business Owners and the TPRM Function to ensure a proper functioning of the TPRM Framework • Support Business Owners in managing Third Party Risk • Oversee the TPRM process for their risk area • Ensure that the relevant Risk Function standards and requirements are contained in the Third Party Code.

TPRM Function	• Define, implement and manage an adequate TPRM Framework and Operating Model together with the Risk Functions, to comply with our TPRM principles • Ensure integration with other relevant functions and processes, e.g. Procurement • Support Business Owners in managing Third Party Risk • Ensure that Third Party risk assessments are carried out as per the Risk Function requirements • Evaluate and propose the inclusion of additional risk areas within the TPRM Framework • Implement and maintain a single technology solution to support the end-to-end risk management process • Deliver the relevant data and information for Risk Function oversight, TPRM management reporting and risk metrics analysis
Procurement (Suppliers only)	• Align with and support the Business Owner on the sourcing approach to be followed for the specific requirement/need and execution, in accordance with the Global Procurement Guideline and associated policies and guidelines, such as the TPRM Guideline • Ensure contract awarding or commitment to suppliers as per the NBS Contracting Requirement Principles, including the TPRM contract clauses as appropriate
• **ERC TPRM Champion**	• Act as a single point of contact (SPOC) at a country/cluster level for TPRM related questions and direct them to the correct function for follow up as required • Support P2P and Business Owners as required in development of meaningful remediation actions relating to Third Parties that have not been risk assessed as per the TPRM non-compliance report • Support local training delivery, including filling any capability gaps in local language or for specific groups (e.g. executives) where required • Escalate issues or challenges faced by country/cluster stakeholder groups during completion of relevant TPRM activities to the TPRM Function

4 Implementation

4.1 Training

Associates must familiarize themselves with this guideline. In addition, they shall be trained in line with the Novartis-wide compliance training curriculum. Additional training, as required, must be undertaken by the Risk and TPRM functions (supported by the TPRM Champion) within their respective organizations.

4.2 Breaches

In alignment with our Code of Ethics, breaches of our policies and guidelines or local laws will result in remedial, corrective or disciplinary actions up to and including termination of employment. Actual or suspected incidents of misconduct should be reported to the SpeakUp Office. Novartis guarantees non-retaliation and confidentiality, to the extent legally possible, for good-faith reports of such breaches.

4.3 Entry into Force and Implementation

This guideline becomes effective 1 October 2020 and replaces the Novartis TPRM Handbook. It must be implemented by all divisions, business units, organizational units, functions and country organizations.

The owner of this guideline is Ethics, Risk and Compliance.

5 Definitions

Business Owner

The Business Owner (in a TPRM context) is the associate who holds the relationship with a Third Party and who is responsible for the business impact of the transaction with the Third Party. The Business Owner therefore assumes and owns any risk(s) identified with the Third Party during the Third Party risk assessment process, as well as during the entire Third Party relationship lifecycle.

No-Go criteria

A “No-Go” is a red line for the organization, as defined by the Risk Functions, which represents an unacceptable or un-mitigatable risk. Novartis will not do business with Third Parties triggering a No-Go (e.g. Third Parties employing child labor).

Risk Function

The functional unit (e.g. Labor Rights, Anti-Bribery, Animal Welfare) responsible for defining the risk policy (e.g. the risk definition, risk position, risk assessment process steps, risk indicators, No-Go criteria, escalation process) relating to their specific risk area.

Third Party

An external natural or legal person or entity outside the Novartis Group and its affiliates.

Third Party Risk Management

The process by which Novartis manages interactions with Third Parties for the purpose of assessing and monitoring the ongoing risk that each Third Party relationship represents.

TPRM Framework

The mandatory framework by which Novartis manages risks relating to Third Parties. It is operationalized through the TPRM operating model.

TPRM Function

The functional unit within ERC, which governs and monitors the TPRM Framework and which liaises with the Risk Functions to ensure that the TPRM Framework is fit for purpose.

Transaction

An interaction with a Third Party resulting in a business impact, which is documented through a Formal Written Contract, Purchase Order or other authorized means with the Third Party.

6 References

ERC Charter

Third Party Code

Risk Function GOPs

TPRM Global Working Instructions

NBS Contracting Requirement Principles