INDEX

INTRODUCTION:

This manual describes the risk management methodology for procuring goods and services provided by third parties at RIMAC SEGUROS, in accordance with the regulations of the Superintendencia de Banca, Seguros y Administradoras de Fondos de Pensiones on the procurement of goods and services provided by third parties, as well as aligned with the principles, framework and risk management process of ISO 31000.

Likewise, this manual is grounded in the Third-Party Risk Management Policy, which sets out guidelines for the efficient and secure acquisition of goods and services, in order to manage spend and Third-Party risk exposure.

Through this methodology, RIMAC SEGUROS seeks to strengthen its capacity to identify, assess, mitigate and monitor the risks associated with contracting third parties, promoting practices that contribute to transparency and operational soundness. The approach addresses both prevention and the proactive management of incidents, ensuring that processes are consistent with international best practices and with the regulatory requirements demanded by local authorities.

The manual provides a clear structure for implementing and overseeing controls, as well as for the periodic assessment of emerging risks arising from third-party relationships. It fosters an organizational culture oriented toward continuous improvement and regulatory compliance, enabling RIMAC SEGUROS to maintain high standards in the responsible management of its suppliers and strategic partners.

1. OBJECTIVE

1.1. Establish the methodology underpinning Third-Party Risk Management in order to minimize risks in the contractual relationship with third parties.

1.2. Define a comprehensive structure providing guidelines for the governance, communication and reporting related to third-party risk management.

1.3. Define roles and responsibilities to ensure adequate governance in the implementation of third-party risk management.

1.4. Establish the structure for documentation related to third-party risk management, including: reports and metrics required for monitoring and managing a third party's incidents.

2. SCOPE

The methodologies, processes and procedures developed and/or derived from this document apply to all RIMAC personnel.
The scope of the manual applies to all Rimac divisions and areas and focuses on the following modalities for procuring goods or services:

- Purchases Over S/. 15,000.00
- Direct Award (direct purchase by exception or simple quotation)
- Purchases Less Than or Equal to S/. 15,000.00 (if the contract or service order does not exceed 30 days / Non-renewable)
- Non-domiciled Suppliers

Third-Party Risk Management (TPRM) Cycle

All Divisions and areas of Rimac must follow the scope of the manual and comply with all the stages of:

- Governance, oversight and management reporting
- Third-party risk management structure / methodology
- Contract
- Ongoing monitoring
- Incident Management
- Exit strategy

3. LEGAL BASIS

- **SBS Resolution No. 272-2017 Corporate Governance and Comprehensive Risk Management Regulation.**
- **SBS Resolution No. 2116-2009 Operational Risk Management Regulation.**
- **SBS Resolution No. 504-2021 Information Security and Cybersecurity Management Regulation.**
- **SBS Resolution No. 789-2018 Standard for the prevention of ML/TF applicable to entities subject to UIF-Peru supervision regarding ML/TF prevention.**

4. DEFINITIONS

- **Third Parties: Individuals or legal entities with whom an agreement or contractual relationship is established related to the acquisition of goods and/or provision of services, grouped as follows:**
  - **Suppliers: Individuals or legal entities with whom there is a contractual relationship and/or agreement for the acquisition of goods and/or provision of services to the Company.**
  - **Counterparties: Individuals or legal entities with whom there is a contractual relationship and/or agreement, and which are not related to the acquisition of goods or provision of services, such as commercial alliances, investment intermediaries, payment services companies, among others.**
  - **Other counterparties: Other counterparties are considered to be individuals or legal entities with whom a contractual relationship and/or agreement is maintained, and which are related to specific activities such as: leases or "fincas" (farm properties), rentals, salvage, real estate investments.**
    Note: Public utility companies, government entities, subscriptions to physical and digital magazines, petty cash reimbursements and commission payments to financial institutions; these counterparties are not within the scope of this policy
- **Third-party risk: The potential for an event, arising from the relationship or interaction with a third party, to negatively affect the organization.**
- **Risk Classification: Third parties must be classified according to the risk they represent, considering criteria such as: criticality of the contracted service, economic value, service offering, supplier solvency, access to sensitive information, impact on technology infrastructure, operational continuity, aspects related to compliance and AML/CFT programs: free competition, personal data protection, money laundering, corporate integrity, anti-corruption, conflict of interest and prevention of market abuse.**

Risks associated with a third-party relationship can be classified as: Operational, Technological, Information Security, Business Continuity, Money Laundering, Corruption, Regulatory Compliance risks, among others.

- **Risk Levels: Risk levels represent the likelihood and potential impact of an undesired event occurring, and are classified as: Low, Medium, High and Extreme.**
- **Risk Assessment: The process of identifying, analyzing and evaluating the risks associated with a relationship with a third party.**
- **Outsourcing: A modality whereby a company contracts a supplier (third party) to deliver goods and/or services that could otherwise be developed by the company itself.**
- **Significant Outsourcing: considered significant when the goods and/or services provided by third parties, in the event of failure or suspension, may pose a significant risk to the company by affecting its revenue, solvency, operational continuity, regulatory compliance**
  or reputation.
- **Due Diligence: Defines the assessment criteria detailing the factors to be considered when assessing a third party, such as its reputation, financial soundness, regulatory compliance, AML/CFT, among others.**
- **Risk Analysis: the process of identifying and assessing the potential risks associated with each third party prior to contracting.**
- **Contracts: A contractual document establishing the business relationship with the third party, which must contain key clauses that mitigate risks, such as penalties for non-compliance, confidentiality agreements, information security and clear responsibilities, among others.**
- **Business Impact Analysis (BIA): The process by which the effects of a business interruption event are assessed to determine the priority with which the Company's processes must be recovered.**
- **AML/CFT: Money Laundering and Terrorist Financing.**
- **TPRM: Third-Party Risk Management**
- **Goods and services: Tangible objects (goods) and intangible objects (services) that have value and are acquired because they are necessary for the Company's operations. They can be classified as: services, merchandise and fixed assets.**
- **GIR Committee: Comprehensive Risk Management Committee**
- **OR: Operational Risk**
- **TechR: Technology Risk**

5. GOVERNANCE (AREAS, POSITIONS/ROLES AND RESPONSIBILITIES)

This section describes the governance model for managing and overseeing third-party risk at Rimac Seguros, detailing roles, procedures, organization, reporting, training, communications and stakeholder relations.

5.1. Third-Party Risk Management Governance Structure

Third-party risk management is organized into three lines of defense, illustrated in the following figure:

Governance Structure of the Third-Party Risk Management Framework

1st Line of Defense	**User Areas**		
	Talent Division	Transformation Division	IT Data Division
	Personal Insurance Division	Corporate Insurance Division	Health Division
	Legal Division	Finance Division	Investments Division
	Information Security1		
2nd Line of Defense	**TPRM Risk and Control Areas**		
	Operational Risk	Business Continuity	Compliance (Compliance and AML/CFT Program)2
	Technology and Data Risk	Legal	Supplier Management /Procurement
3rd Line of Defense	**3rd Line of Defense**		
	Internal Audit		

5.1.1. First Line of Defense – User Areas

All user areas that require the procurement of goods or services constitute the first line of defense, and are responsible for implementing internal controls and practices aligned with the third-party risk management policy. This is intended to enable informed decisions on risk and return in procurement processes.

1 The third-party risk assessment in the information security area is carried out by the Security Governance team.

2 Compliance and AML/CFT programs: Free competition, personal data protection, money laundering, corporate integrity, anti-corruption, conflict of interest and prevention of market abuse.

Implementing the third-party risk management policy is the responsibility of all Rimac areas, teams and/or employees involved in establishing or maintaining relationships with third parties. In coordination with their supplier, they must ensure compliance with the control actions arising from the risk assessment in the procurement of goods or services from third parties.

Information Security Area

Responsible for identifying, assessing and treating risks associated with the contractual relationship with Third Parties regarding the handling of information. It assesses the level of assurance over information and/or data shared with the supplier under the principles of confidentiality, integrity, availability, authentication, authorization and non-repudiation, as the first line of defense.

5.1.2. Second Line of Defense – TPRM Risk and Control Areas:

The Operational Risk, Business Continuity, Compliance (Compliance and AML/CFT Program), Technology and Data Risk, Supplier Management/Procurement and Legal areas; these areas constitute the Second Line of Defense within the third-party risk management framework and are responsible for assessing the risks associated with the procurement of goods and/or services, as indicated below:

a. Operational Risk Area

The Operational Risk area is responsible for drafting the third-party risk management policy and the procedures for implementing this policy.
Likewise, it is responsible for updating it according to business needs and for identifying, assessing and treating the operational risks that may result from the contractual relationship with a third party.

b. Business Continuity Area:

The Business Continuity area is responsible for assessing whether the good or service provided by the Third Party is essential to the operational continuity of any of the critical processes mapped in Rimac's BIA.

c. Technology and Data Risk Area

Responsible for assessing whether the supplier, with respect to the contracted service, has a significant impact on the availability of Rimac's technology assets and data quality, considering the following aspects:

- The nature and criticality of the systems, platforms or data sources involved, especially those that support critical operations
- The degree of integration with core systems or critical data flows.
- The level of exposure to technology risks, such as data availability and quality."

d. Compliance Area

Responsible for identifying, assessing and treating risks associated with the contractual relationship with Third Parties on matters related to the Compliance programs: AML/CFT, Corporate Integrity (anti-corruption, conflicts of interest), Prevention of market abuse, free competition and personal data protection, and any other applicable program.

e. **Supplier Management / Procurement Area**

Responsible for identifying, assessing and treating risks associated with the following aspects:

- **Economic Value: Represents the risk assessment regarding the average annual payment to the supplier for the contracted goods and/or services, based on the segmentation performed under the Procurement area's risk framework.**
- **Service Offering: Represents the assessment of the diversity of the market's offering for the contracted and/or subcontracted good or service. Represents the assessment of the shortlist of suppliers.**
- **Solvency: Represents the assessment of the supplier's financial soundness and level of indebtedness.**

f. **Legal Area**

Responsible for drafting the contract / addenda / service order / and/or commercial agreements with a third party for the procurement of a good or service; these contractual documents must contain clauses that support third-party risk management for suppliers with critical and/or significant services with high risk exposure.

In the case of services provided by third parties in matters relating to information technology management, information security management or data processing, the Legal area must ensure that the contractual arrangement with the supplier and its implementation enable compliance with the obligations set out in the Comprehensive Risk Management Regulation and the Information Security and Cybersecurity Management Regulation, and must establish the roles and responsibilities the supplier contractually assumes under these regulations.

Responsible for including in contracts with Third Parties (including Consultants) clauses that guarantee compliance with Rimac's internal policies, such as travel and per diem policies, among others, in order to have a control that minimizes exposure to financial losses and reputational risk arising from the behavior of a third party.

Responsible for implementing the exit strategy for the contractual relationship with the Third Party and ensuring the service level agreements with the Supplier are included in the contract, as applicable.

g. **Occupational Health and Safety Area**

Responsible for identifying, assessing and treating risks associated with the contractual relationship with Third Parties in relation to the occupational health and safety program

5.1.3. Third Line of Defense – Internal Audit

Internal Audit is considered the third line of defense in third-party risk management, performing tests, verifying the correct use of controls related to third-party risk management in compliance with internal policy, and also measuring the effectiveness of its implementation.

5.2. RACI Matrix

The RACI matrix is a tool that clarifies the roles and responsibilities of each team for specific tasks, using a chart in which the letters stand for: Responsible, Accountable, Consulted and Informed.

Its objective is to ensure that each task has an area and/or person who executes it, one who approves it, someone to consult for information, and people to be kept informed of progress.

For third-party management it is applied as follows:

Legend							
R	Responsible	**A**	Accountable	**C**	Consulted	**I**	Informed

Third-Party Risk Management (TPRM)	Roles								
	User area	IS	Procurement	Legal	Risk & Compliance Division				GIR Committee
					RO[1]	CN[2]	RTI[3]	Compliance	
Approve the policy and organization for third-party risk management.	I	I	I	I	C	C	C	C	RA
Development of the TPRM policy and procedures manual.	I	CI	CI	CI	R	CI	CI	CI	A
Identify and assess the risks present in the relationship with the third party.	CI	R	R	CI	R	R	R	R	I
Implement treatment plans and control actions.	R	CI	CI	CI	CI	CI	CI	CI	AI
Decide on actions aimed at addressing deviations in risk appetite levels and limits and the degrees of exposure of risk assumed for TPRM.	CI	CI	CI	CI	CI	CI	CI	CI	RA
Notify the Procurement and Risk areas of the need to acquire a good or contract a service.	R	I	I	CI	I	I	I	I	AI
Drafting of the contract / addenda / service order / and/or commercial agreements with a third party.	CI	CI	CI	R	CI	CI	CI	CI	I
Implement the exit strategy for the termination of the contractual relationship with the Third Party.	I	I	I	R	I	I	I	I	I
Monitoring and Follow-up	R	RC	RC	RC	RC	RC	RC	RC	I

[1] RO stands for Operational Risk
[2] CN stands for Business Continuity
[3] RTI refers to Technology Risk

5.3. Reporting Management

The Risk Division is responsible for Third-Party Risk Management at Rimac and must consolidate the information from the assessments performed for the procurement of goods and/or services, providing reports to senior management at the Risk Committees, reporting on key metrics, issues, policy adherence, among other aspects.

Below is a non-exhaustive list of the information that must be reported to the Risk Committee regarding third-party risk management:

- Report on the risk assessment performed on third parties, highlighting the criticality of the supplier and of the contracted service (applicable to significant and/or critical contracting or subcontracting).
- Report on the follow-up of action plans and their degree of compliance by the user areas and their respective suppliers.

5.4. Training and Communication

Stakeholders must receive training on the Third-Party Risk Management policy and manual, as well as become familiar with the requirements, functions, responsibilities and the risk assessment process applicable to suppliers.

Frequent, clear communication with Senior Management, Legal, Procurement and Compliance is required to mitigate risks, demonstrate value, maintain engagement and improve visibility of escalated matters.

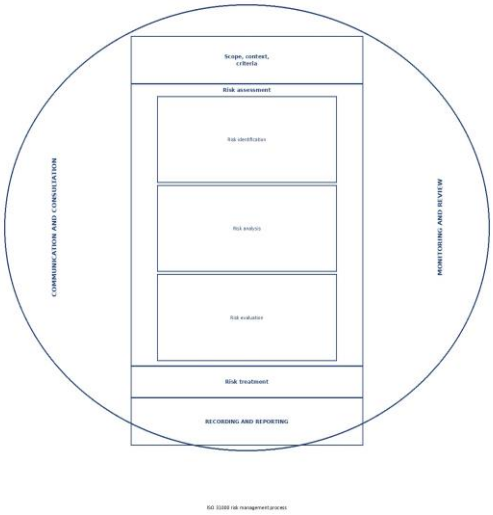
The Third-Party Risk Management manual provides Rimac with an overview of the management framework. The Operational Risk area is responsible for developing, facilitating access to, and conducting the training once a year for the parties involved, as well as for regularly monitoring compliance with the policy and corresponding manual.

6. DEVELOPMENT OF THIRD-PARTY RISK MANAGEMENT METHODOLOGY

RIMAC has developed a methodology that underpins a framework for proper Third-Party Risk Management. In compliance with this, Rimac uses qualitative management models, and their implementation is essential to establish a uniform process through which a comprehensive, proactive approach to reducing third-party risk is structured.

To implement the Third-Party Risk Management methodology, RIMAC aligns with ISO 31000, which establishes a reference framework aimed at helping organizations integrate risk management into all their main activities and functions. To achieve this, the support and commitment of stakeholders is necessary, especially senior management. Developing the reference framework involves integrating, designing, implementing, evaluating and continuously improving risk management across the organization; which we apply to third-party risk management.

The Third-Party Risk Management Methodology is based on the following ISO 31000:2018 process



For Rimac, the internal control environment is the environment that influences the members of the organization and the control of its activities. This environment is the foundation of corporate risk management and third-party risk management, since it provides discipline and structure, and it also affects every component of comprehensive risk management.

Likewise, to implement this methodology Rimac must have human resources standards and establish practices for hiring, onboarding, training, coaching and compensation, which is a fundamental process of the internal control environment. Similarly, the mechanisms and actions to be taken for non-compliance with the rules set out in the third-party risk management policy and procedures manual must be determined.

6.1. METHODOLOGY FOR THIRD-PARTY RISK MANAGEMENT

The third-party risk management methodology at Rimac is based on two stages:

- Phase 1: Assessment of Goods and/or Services
- Phase 2: Third-Party Risk Assessment

6.1.1. Phase 1: Assessment of Goods and/or Services

The assessment of goods and/or services is carried out before selecting and contracting the supplier. This process aims to measure the potential impact on criticality and relevance in the event the good or service is suspended, considering aspects such as revenue, solvency, operational continuity or reputation.

Goods and/or services are those delivered to the company by a supplier, and when it is a good and/or service that could be developed by the company but it decides to request it through a third party instead, this constitutes outsourcing.

Rimac has established a criticality matrix to determine whether a good or service is “Critical” and/or “Significant,” taking into account the following definitions:

- **Critical: A good and/or service is considered critical when its failure or suspension severely affects operations and/or technology and has the highest priority in resilience and business continuity planning.**

- **Significant3: Goods and/or services are considered significant when, in the event of failure or suspension, they may pose a significant risk to the company and affect its revenue, solvency, operational continuity or reputation.**

The Criticality Matrix is intended to determine the "criticality and significance" of the good or service prior to contracting; and thereby prioritize the identification of significant and/or critical suppliers and manage the risks associated with contracting them, specifying cases that fall under the outsourcing modality.

Criticality Matrix for Goods and/or Services

Where:

3 Res. SBS 272-2017. (Chapter IV Art. 35)

Criticality Measurement Table

Quadrant	Description	Action Plan
I CRITICAL + SIGNIFICANT	If the good or service to be contracted has an impact on primary processes4 and/or falls within the critical processes of the Business Impact Analysis (BIA), and its failure or suspension could severely affect5 revenue, and/or solvency, and/or operations, and/or reputation, and/or technology infrastructure, and/or operational continuity, and/or the processing of personal data.	Contracting the supplier requires a comprehensive risk assessment.
II SIGNIFICANT + NOT CRITICAL	If the good or service to be contracted has an impact on a support process and its failure or suspension could pose a significant risk to the company and affect its revenue, solvency, operational continuity or reputation.	Contracting the supplier requires a comprehensive risk assessment.
III NO T SIGNIFICANT	Failure or suspension of the good or service does not affect operations, but may generate a minor risk in some company process.	Does not require a supplier risk assessment, but it does go through Procurement and Crime Prevention filters6.
IV NOT CRITICAL	Failure or suspension of the good or service to be contracted **does not generate risks for the Company.**	Does not require a supplier risk assessment, but it does go through Procurement and Crime Prevention filters.

Likewise, for the assessment of goods and services, Rimac defines the following concepts regarding a failure or suspension that could affect the company in the following aspects:

- Revenue: Impacts Rimac's achievement of results, causing it to fall short of planned targets and affecting the company's revenue.
- **Solvency: Impacts Rimac's ability to meet its financial obligations, or impacts regulatory solvency ratios.**
- **Continuity: Impacts Rimac's business continuity of critical processes.**
- **Operations: Impacts Rimac by delaying operations or causing degradation in the delivery of services to our stakeholders.**

4 Primary Processes: According to the Process Map recorded in Goldenbelt as of August 2025. (1. Community Management and Intelligent Prospecting. / 2. Product and Service Development. / 3. Sales and Renewal. / 4. Policy Management. / 5. Post-Sale Services (Claims and Customer Experience). / 6. Investment Management).

5 According to the Process Map recorded in Goldenbelt as of August 2025. (1. Talent Attraction and Development. / 2. Financial Management. /3. Risk and Audit Management. 4. Legal and Regulatory Support / 5. Supplier and Asset Management. / 6. Data and Analytics Governance (GenAI)./ 7. Technology Development and Operations).

6 Procurement filters consist of running the Third Party through validations for over-indebtedness and negative information reported by all or some of the following entities: Equifax, OSCE, Sunat, ERP and Watchlist.

- **Reputation: Degrades the Company's standing due to opinions based on customer experience (external and/or internal), or the public perception of our stakeholder group.**

Based on the definitions described in the previous paragraph, the user requesting the procurement of a good or service must answer the following questionnaire:

No.	Description	YES	NO
1	Does the good and/or service to be contracted belong to a Primary Process: 1. Community Management and Intelligent Prospecting. / 2. Product and Service Development. / 3. Sales and Renewal. / 4. Policy Management. / 5. Post-Sale Services (Claims and Customer Experience). / 6. Investment Management.		
2	Does the good and/or service to be contracted belong to a Support Process: 1. Talent Attraction and Development. / 2. Financial Management. /3. Risk and Audit Management. 4. Legal and Regulatory Support / 5. Supplier and Asset Management. / 6. Data and Analytics Governance (GenAI)./ 7. Technology Development and Operations.		
3	Could the service be developed by a Rimac area, but for various reasons it has been decided to outsource the activity to a Third Party?		
4	Could the failure or suspension of the good and/or service affect revenue based on the achievement of Rimac's strategic objectives?		
5	Could the failure or suspension of the good and/or service affect Rimac's solvency in meeting its obligations?		
6	Could the failure or suspension of the good and/or service affect the operational continuity of a Rimac process?		
7	Could the failure or suspension of the good and/or service severely affect Rimac's **reputation (*)?** (*) Negative news in the media, social networks, or unrecoverable loss of trust among its suppliers, business partners, external or internal customers?		
8	Is the good and/or service to be contracted related to data processing, and/or cloud services?		
9	For the implementation of the good or service to be contracted, must the supplier use information associated with sensitive data (biometric data, genetic data, facts or circumstances of one's emotional or family life, personal habits belonging to the most intimate sphere, information relating to union membership, physical or mental health, or other similar information affecting one's privacy)?		
10	Could the failure of the good or service expose Rimac to regulatory non-compliance?		

The result of the questionnaire will determine which quadrant of the criticality matrix the good or service to be contracted falls into, as detailed below:

Comprehensive Risk Assessment		Procurement / Crime Prevention Filters	
Questionnaire Result - Criticality of the Good or Service			
I Critical and Significant	II Significant	III Not Significant	IV Not Critical
YES marked on items: 1 and at least on one of questions 3 through 10	YES marked on items: 2 and at least on one of questions 3 through 7	YES marked on items: 1 or 2 and at least on one of questions 3, 9 and 10	YES marked on items: 1 or 2 and the rest of questions marked NO.

Goods and/or services located in quadrants I and II mandatorily require the risk assessment of the supplier selected for their procurement.

For critical and/or significant goods or services (Quadrants I and II), Rimac must consider at least the following aspects for contracting the supplier:

a. Implement a supplier selection process for the good and/or service, in accordance with what is established in the procurement and supplier management contracting policies.
b. Have a contract, which must include service level agreements; clearly establish the responsibilities of the supplier and the company;
c. Establish in the contract the jurisdiction that will prevail in the event of a conflict between the parties;
d. Incorporate the required information security levels into the contract (where applicable).
e. Include exit strategies in the contract.
f. In the case of significant outsourcing, clauses must be included that facilitate an adequate review of the respective service by the companies, by the internal audit unit, by the external audit firm, as well as by the Superintendencia.
g. Include regulatory clauses on: information security, operational risk, business continuity, crime prevention and personal data processing.
h. Manage and monitor the risks associated with these services.

6.1.2. Phase 2: Third-Party Risk Assessment

Third-party risk assessment is a structured process to identify, assess, mitigate and monitor risks associated with suppliers when contracting critical and/or significant goods or services.

The company must carry out an assessment of the risks associated with significant services provided by third parties, whether or not they fall under the outsourcing modality. Such assessment must be submitted to the board of directors for approval.7

7 Res. SBS 272-2017. (Chapter IV Art. 36)

This phase applies to the procurement of critical and/or significant goods and/or services, which must go through review and assessment by the following areas:

- **Procurement: Area responsible for running supplier filters for procurement segmentation based on economic value, service offering and solvency.**
- **Information Security: Assesses the level of assurance regarding information and/or data shared with the supplier under the principles of confidentiality, integrity, availability, authentication, authorization and non-repudiation.**
- **Operational Risk: Assesses the operational risks related to the contracted good or service, associated with human resource, process, technology or external factors.**
- **Technology and Data Risk: Assesses the risks associated with the technology and data provided by the contracted supplier as part of its service.**
- **Compliance: Assesses the supplier on matters related to AML/CFT, Corruption, Conflicts of Interest, Market Abuse, corporate integrity, among others.**
- **Business Continuity: Assesses whether the good or service provided by the Third Party is essential to the operational continuity of any of the critical processes mapped in Rimac's BIA.**

These areas are responsible for the Supplier's risk assessment, and will determine the level of risk exposure according to the following assessed criteria:

Phase II - Third-Party Risk Assessment Criteria				
Governance/ Owners	**Criterion Assessed**	**Description**	**Detail**	**Risk Level**
Procurement	Economic Value	Represents the average annual payment to the supplier for the contracted goods and/or services, based on the segmentation performed under the Procurement area's risk framework.	**Transactional: Suppliers that fulfill specific orders without necessarily establishing a long-term relationship.** They have a low impact on the business and annual billing exceeds USD 500K	Low
			Foundational: Suppliers essential to the basic functioning of the business, due to the high volume of needs they meet. They have a low impact on the business and annual billing exceeds USD 500K.	Medium
			Niche: Highly specialized suppliers, but with limited scope. They have a high impact on the business and have annual billing below USD 500K.	High
			Strategic: Suppliers with whom the relationship and collaboration generate a long-term competitive advantage, and with whom alliances are sought. They have a high impact on the business and have annual billing above USD 500K.	Extreme
	Service Offering	Assesses the diversity of the offering for the good or	**Multiple suppliers in the market: There are many suppliers in the market to contract the good and/or service,**	Low

Phase II - Third-Party Risk Assessment Criteria				
Governance/ Owners	**Criterion Assessed**	**Description**	**Detail**	**Risk Level**
		contracted and/or subcontracted service in the market. Represents the assessment of the shortlist of suppliers.	**Few suppliers in the market: There are few suppliers in the market to contract the good and/or service.**	Medium
			Sole supplier in the market: the only supplier nationwide that offers the good or service to be contracted.	High
			Direct Award: Acquisitions exempted from the requirement to present more than one quotation or to evaluate a shortlist of suppliers.	Extreme
	Solvency	Assesses the supplier's financial soundness in meeting its obligations and its level of indebtedness, based on: tax delinquencies, outstanding debts, Equifax, OSCE, Watchlist, ERP.	The company does NOT present negative information and demonstrates financial solvency and soundness that guarantees contractual compliance with Rimac regarding delivery of the contracted good or service,	Low
			The company shows over-indebtedness and negative information reported in all or some of these Entities: Equifax, OSCE, Sunat, ERP and Watchlist.	High
Business Continuity	Operational Continuity	Assesses whether the good or service provided by the Third Party is essential to the operational continuity of any of the critical processes mapped in the Rimac BIA.	**Not Critical:** The service provided by the supplier is not directly related to a critical process of the area (as obtained from the BIA).	Low
			Critical: The service provided by the supplier is directly related to a critical process of the area (as obtained from the BIA). Bear in mind that interruption of this service will directly affect business continuity.	High
Operational Risk	Contracted Service	Assesses whether the good and/or service is significant and/or critical, considering that in the event of failure or suspension, it may pose a significant risk to the company or severely affect its revenue, solvency, operational continuity or reputation.	**Not Critical** Failure or suspension of the good or service to be contracted does not generate risks for the Company.	Low
			Not Significant: Failure or suspension of the good or service does not affect operational continuity, but may generate a minor risk in some company process.	Medium
			Significant and Not Critical: If the good or service to be contracted has an impact on a support process and its failure or suspension may pose a significant risk to the company and affect its revenue, solvency, operational continuity or reputation, as well as personal data processing.	High
			Critical and Significant: If the good or service to be contracted has an impact on primary processes and/or falls within the critical processes of the Business Impact Analysis (BIA), and its failure or suspension may severely affect revenue, and/or solvency, and/or operations, and/or reputation, and/or technology infrastructure, and/or business continuity, and/or personal data processing.	Extreme
Technology Risk	Technology / Data	Assesses whether the supplier, with respect to the service	**System purchase or lease service (SaaS):** - the application will not integrate with any additional system and covers one (1) business process (does not include a critical process).	Low

Phase II - Third-Party Risk Assessment Criteria				
Governance/ Owners	**Criterion Assessed**	**Description**	**Detail**	**Risk Level**
		contracted, has a significant impact on the availability of Rimac's technology assets and data quality, considering the following aspects:	**System purchase or lease service (SaaS):** - the application will not integrate with any additional system and covers some business processes (does not include a critical process). IT operation or support service: - will provide maintenance, development or QA testing service covering one (1) system and several business processes (service is not cross-cutting). **Data or information purchase service:** - Data or information will serve as input to operate commercial processes.	Medium
			System purchase or lease service (SaaS): - the application will integrate with several systems and covers several business processes. **IT operation or support service:** - will provide maintenance, development or QA testing service on a cross-cutting basis or covering several systems and several business processes (including some critical ones). **Data or information purchase service:** - Data or information will serve as input to operate critical processes.	High
			System development, purchase or lease service (SaaS): - the application will integrate with core systems and covers several critical business processes. **IT operation or support service:** - will provide infrastructure support (on-premises or cloud), IT operation or support (access, change, incident and backup management), and is also identified in the current Application Impact Analysis (AIA). **Data or information purchase service:** - Data or information will serve as input to generate regulatory reports.	Extreme
Information Security	Information Security	Assesses the level of assurance regarding information and/or data shared with the supplier under the principles of confidentiality, integrity, availability, authentication, authorization and non-repudiation.	The supplier does NOT use personal data, health data or contact data. The supplier does NOT manage information that could compromise RIMAC's operations or reputation. The product or service delivered will NOT connect to or interact with RIMAC's core technology infrastructure, corporate networks or critical systems, and has NO bearing on the operational continuity of the business; the product or service provided is NOT related to core critical business processes.	Low
			The supplier uses personal data, health data or contact data; the product or service provided by the supplier has a bearing on operational continuity.	High
			The supplier uses personal data, health data or contact data. The supplier manages information that could compromise RIMAC's operations or reputation, the product or service provided by the supplier will connect to and interact with RIMAC's core technology infrastructure, corporate networks or critical systems.	Extreme Extreme

Phase II - Third-Party Risk Assessment Criteria				
Governance/ Owners	**Criterion Assessed**	**Description**	**Detail**	**Risk Level**
			The supplier uses personal data, health data or contact data. The supplier manages information that could compromise RIMAC's operations or reputation, the product or service provided by the supplier will connect to and interact with RIMAC's core technology infrastructure, corporate networks or critical systems, and has a bearing on the operational continuity of the business, and the product or service is also related to core business critical processes.	
Compliance Management	Compliance	Assesses the level of acceptance based on the review carried out by the compliance area on matters related to AML/CFT, Corruption, Conflicts of Interest, Market Abuse, Free Competition, Corporate Integrity, Personal Data Protection	**Corporate Integrity:** The supplier, or any of its shareholders (+>10%) and/or legal representatives, is a public official or Politically Exposed Person (PEP).	Low
			AML/CFT: - The supplier is local and operates in a high-risk area; or - The supplier, or any of its shareholders (+>10%) and/or legal representatives, is registered on a Yellowlist; or - It operates, works or provides services related to a low-risk sales channel; or - The economic activity offered by the supplier is medium risk; or **Corporate Integrity:** - During the performance of the service the supplier will interact with a public official; or **PADM (Market Abuse Prevention):** - The supplier provides external financial audit services	Medium
			Corporate Integrity: - During the performance of the service the supplier will represent Rimac before a public official or will carry out some procedure with government entities, or - The supplier has an apparent, potential or real conflict of interest in providing the service, or **PADM:** - The supplier has access to privileged information **Free competition:** - The supplier requires exclusivity from RIMAC, preventing other suppliers from providing the same service. - The supplier accepts contractual conditions that limit its freedom to contract with other companies.	High
			AML/CFT: - The supplier is from a foreign country; or - The supplier, or any of its shareholders (+>10%) and/or legal representatives, is registered on a Blacklist; or - It operates, works or provides services in a medium- or high-risk sales channel; or - The supplier's economic activity is high risk; or **Corporate Integrity** The supplier, or any of its shareholders (+>10%) and/or legal representatives, has a criminal record or is under investigation or sanction for cases of Corruption, tax fraud, off-the-books accounting or offenses against cultural heritage, ML/TF or predicate offenses; or **PADM:** The supplier has access to privileged information and provides placement or brokerage services in the securities market.	Extreme

Phase II - Third-Party Risk Assessment Criteria				
Governance/ Owners	**Criterion Assessed**	**Description**	**Detail**	**Risk Level**
			Free competition: - The supplier will manage RIMAC's sensitive commercial information (future premium or policy pricing, cost structure, business strategy, among others) and also works with competitors. - The supplier receives benefits or incentives from RIMAC for not contracting with competitors.	

6.1.2.1. **Criteria to Consider for Risk Assessment:**

All areas involved in the Third Party's risk assessment shall apply the stages of risk identification, assessment, treatment and control in their evaluation, aligned as a standard with the "Methodology for Assessing Operational Risks and Controls" described in the operational risk manual.

1. **Risk Identification**

   The identification of risks associated with contracting a Third Party for significant and/or critical goods and/or services seeks to find, recognize and describe the risks that may affect the achievement of Rimac's objectives, both internally and externally, as a result of a contractual relationship with a Third Party, which may have a reputational, financial or regulatory impact and may also erode our customers' trust

   The following structure will be used to record identified risks:

N	Name	Description
1	Operational risk code	Unique code assigned by the company to identify the operational risk
2	Service identifier	Unique code assigned by the company to identify the service; if none exists, indicate the sequential number assigned in table 1
3	Risk identification date	Date on which the company identified the risk (Format DD/MM/YYYY)
4	Operational risk factor	1: Inadequate or deficient internal processes 2: Personnel failures 3: Information systems failures 4: External events
5	Company Product/Service	Company product/service where the operational risk was identified (see table 1)
6	Channel	Channel where the operational risk was identified
7	Process	Process where the operational risk was identified
8	Level 1 event type	Classification of the event type at level 1, according to the types indicated in Annex No. 3 of SBS Resolution No. 2116-2009
9	Level 1 business line	Classification of the business line at level 1, according to the lines indicated in Annex No. 4 of SBS Resolution No. 2116-2009
10	Residual risk frequency	Frequency or probability of occurrence of the risk
11	Residual risk impact	Estimated monetary impact of the individual materialization of the risk
12	Residual risk level	Risk level resulting from the assessment process, considering controls
13	Risk response	Record the process chosen: 1: Accept the risk 2: Decrease the probability of occurrence 3: Decrease the impact 4: Transfer partially 5: Transfer fully 6: Avoid it 7: Combination of the above measures 8: Other
14	Date of last review	Date on which the company performed the last review or update of the risk assessment (Format DD/MM/YYYY)

2. Risk Assessment

This section covers the assessment of inherent risk; the internal control environment is evaluated by measuring the design of current controls, their performance and effectiveness in mitigating risk, thereby obtaining the residual risk exposure. For recording purposes, the risk assessment section of the Toolkit_RCSA_V2.1, used for assessing risks and controls in processes, will be used as a reference.

Risk Assessment					Inherent Risk
	Inherent Frequency: An event occurs...	Frequency rationale: Example: Indicate what drivers were taken into account to estimate the frequency.	Inherent Impact	Rationale for the significant impact(s)	Inherent Risk Level
Very Frequent	More than 12 times per year		Discontinuity of ≤ 4 hours or absorbable under normal operating conditions	Insignificant	MEDIUM

...

	Internal Control Environment	Control Design Assessment										Control Performance Assessment			
#	Description of Controls	Natural	0.25	Documented	0.15	Evidence	0.15	Type	0.25	Periodicity	0.25	Design Result	Mitig. Frequency	Perf. Rating	Mitig. Impact	Perf. Rating
C1	The Vehicular Persons team cross-checks information between renewal policies and new-sale policies. It validates coincidences in fields such as serial number, plate, engine and customer ID number, with the aim of identifying cases where a renewal policy has been cancelled and issued as a new sale.	Manual	0.3	Not Documented	0	Leaves Evidence	1	Detective	0.5	Regular	0.5	44%	Null	0%	Acceptable	50%

Impact Typology

Impact Typology	Catastrophic	Major	Moderate	Minor	Insignificant
Customers	Severe impact disabling a broad range of customers, products, systems, operations and/or internal staff	Significant impact on customers, products, systems, operations and/or internal staff	Moderate impact on customers, products, systems, operations and/or internal staff	Minor impact on customers, products, systems, operations and/or internal staff	Minimal impact on customers, products, systems, operations and/or internal staff
Financial	Impact greater than 1% of equity (>=USD 7M)	Impact between 0.1% and 1% of equity (USD 700K < 7M)	Impact between 0.05% and 0.1% of equity (USD 350k < 700K)	Impact between 0.01% and 0.05% of equity (USD 70K < 350K)	Impact equal to or less than 0.01% of equity (<USD70k)
Regulatory - Legal	Impact on the license or authorization to operate, or major non-compliance with significant sanction	Relevant non-compliance with critical observations by the regulator or sanction	Moderate non-compliance with formal observations by the regulated entity	Minor non-compliance without sanction, with minor improvement recommendations	Full compliance with no observations or regulatory impact
Reputational	Significant negative external headlines, with strong mention in the media and/or major impact on consumers	Important negative headlines in the media and/or reputational impact with considerable visibility	Moderate negative headlines with some media visibility and/or moderate impact on consumer perception	Minor negative headlines or slight and limited impact on consumers	Negligible impact, no relevant mention in the media nor damage to public perception
Continuity of Business	Downtime greater than the process/product's MTPD	Downtime equal to the process/product's MTPD	Downtime less than the process/product's RTO	Downtime less than the process/product's RTO	Minimal incidence that does not affect the functioning of the process/product

3. **Risk Treatment**

In this section, the response to risks associated with Third Parties whose residual risk exposure falls outside our appetite and tolerance is planned; strategies are assessed to: Reduce, Transfer, Accept and/or Increase them.

Action Strategy	
Accept	Accept the identified risk without taking additional action, when its impact is low or its mitigation is not feasible.
Reduce	Implement measures to decrease the probability or impact of the risk.
Transfer	Fully or partially delegate the risk to a third party through contracts, insurance or other mechanisms.
Increase	Accept a higher level of risk in order to take advantage of an opportunity or achieve a greater benefit.

For recording purposes, the risk response section of the Toolkit_RCSA_V2.1, used for assessing risks and controls in processes, will be used as a reference.

Residual Risk			Response	
Residual Frequency	Impact Residual	Residual Risk	Strategy	Initial A.P. (Proposal)
Very Frequent	Insignificant	MEDIUM	Reduce	

Likewise, controls must have the following characteristics:

N	Name	Description
1	Control code	Unique code assigned by the company to identify the control
2	Operational risk code	Unique code assigned by the company to identify the operational risk indicated in table No. 2
3	Description	Description of the control
4	Type	1: Preventive 2: Detective 3: Corrective
5	Effect	1: On frequency 2: On impact 3: On frequency and impact
6	Date of last review	Date on which the company performed the last review or update of the control assessment (Format DD/MM/YYYY)

4. Risk Control

This section establishes action plans to mitigate “unacceptable” risks, assigning owners and implementation dates.

Once Third-Party risks with High or Extreme risk exposure have been identified, and new control actions have been proposed in response to the risk, the decision to implement them lies with the various business units, who are responsible for requesting the contracting of the good or service, and who must contact the Third Party to define implementation dates.

The maximum time frames for executing the control actions set out in the supplier's risk assessment must be met according to the implementation date agreed with the business unit responsible for the contracting.

Likewise, the guidelines for managing action plans are included in the Issue Management policy.

An action plan matrix must be established considering the following fields:

Fields	Description
Action plan code	Unique code assigned by the company to identify the action plan.
Approval date	Date on which the company approved the treatment measure in response to the risk (Format DD/MM/YYYY).
Operational risk code	Unique code assigned by the company to identify the operational risk.
Description	Description of the action plan.
Owner	Person responsible for implementing the action plan.
Scheduled implementation date	Implementation date scheduled at the time the action plan was approved (Format DD/MM/YYYY).
Actual implementation date	Final date on which implementation of the action plan was completed (Format DD/MM/YYYY).
Extensions	Number of times the action plan's implementation date was modified in order to extend the scheduled date
Status	1: Pending: in the process of being implemented 2: Implemented: implementation has been completed.

6.2. Monitoring and Follow-up

The purpose of monitoring and follow-up is to ensure the implementation of control actions and is also essential for detecting changes in a Third Party's risk profile.
Rimac establishes the following mechanisms to assess compliance with third-party risk management, based on the following guidelines:

- The Business Unit Leader who requests the contracting of the significant good or service is responsible for monitoring compliance with the service level agreement bimonthly and reporting any non-compliance to the Procurement, Legal and Operational Risk areas so that the corresponding actions can be taken as set out in the contract.

- As part of following up on control actions, Third Parties with a High risk exposure and/or that are Significant or higher must have a contract containing service level agreements (SLAs) that guarantee the operational continuity of the contracted good and/or service, and must also contain regulatory clauses on operational risk, business continuity, information security and money laundering that facilitate a proper review of the respective service delivery by the internal audit area.

- In the event of any incident, occurrence or interruption of the contracted good or service, the business unit that contracted the good and/or service must report the incident to the risk area and the legal area so that they can validate compliance with the established service level agreements and assess whether a penalty should apply, and also consider it as an operational event, if applicable.

- The Regulatory Compliance area is responsible for ensuring compliance with the policy and the Third-Party Risk Management manual.

- Establish key performance indicators (KPIs) to assess proper delivery of the service, as well as the Third Party's quality and compliance with the user area that contracted the good and/or service.

- Request periodic reports and follow up on the services provided.

- Update the initial risk assessment performed on the Third Party based on new events, incidents or regulatory changes.

- Foster open communication and voluntary incident reporting by the Third Party.

Non-Compliance Reports:

The Supplier Management and Procurement area is responsible for notifying user areas when they fail to comply with the Third-Party Risk Management Policy; such notification will be sent as soon as it is identified that a policy guideline is not being met, and will generally be flagged through an email that will include the reason for the non-compliance.

Below is a list of the types of non-compliance that may be observed:

- The supplier contracted for critical and/or significant goods or services did not go through the risk assessment.
- There are no service level agreements in the contract for a critical and/or significant good.
- Control actions set out in the supplier's risk matrix are not being met
- Incidents regarding the efficiency of delivery of the service contracted to the supplier are not being reported.
- There is no monitoring of service level agreements by the area.
- There are no signed, updated and/or safeguarded contracts.

    - The Supplier Management and Procurement area will track the percentage of non-compliant activities by each user area so that corrective measures can be taken. The Non-Compliance Report, identifying the users involved, in order to foster adherence to the policy, will be reported to the Division's VP once the event is identified.
    - If a user area appears in the policy non-compliance report 3 times, it must complete in-person training with the Risk and Supplier and Procurement Management team. If it continues to appear in the non-compliance report, it will be reported to Internal Audit and Talent.
    - A non-compliance report will be sent bimonthly to the risk division for presentation to the GIR Committee.

6.3. Key Performance Indicators (KPIs)

Key performance indicators (KPIs) will be established for Third Parties with High or Extreme risk exposure, to monitor the Third Party's quality and compliance with the user area that contracted the good and/or service, considering the following criteria:

- **Relevance: KPIs must be directly related to the services provided by the third party and the associated risks.**
- **Measurability: They must be quantifiable and have reliable data sources.**
- **Frequency: They must have a defined measurement frequency (monthly, quarterly, etc.).**
- **Accountability: Each KPI must have an owner responsible for follow-up and reporting.**

The user area is responsible for establishing the indicator and carrying out the corresponding monitoring. Indicators must be associated with:

1. **Operational Performance**
    - SLA (Service Level Agreement) compliance level.
    - Response and resolution times.
    - Service availability.

2. **Incident Management**
    - Number of incidents reported.
    - Average incident resolution time.
    - Results of audits or reviews.

3. **Regulatory Compliance**
    - Updating of legal and technical documentation.

4. **Internal User Satisfaction**
   - Satisfaction surveys.
   - Qualitative feedback from the user area.

5. **Continuity and Resilience**
   - Execution of continuity tests.
   - Results of drills or contingency exercises.

7. SOURCING AND DUE DILIGENCE

Sourcing consists of selecting a third party through due diligence methods. The selection strategy varies according to risk, purchase complexity and the type of supplier (sole, renewal, or new to the market).

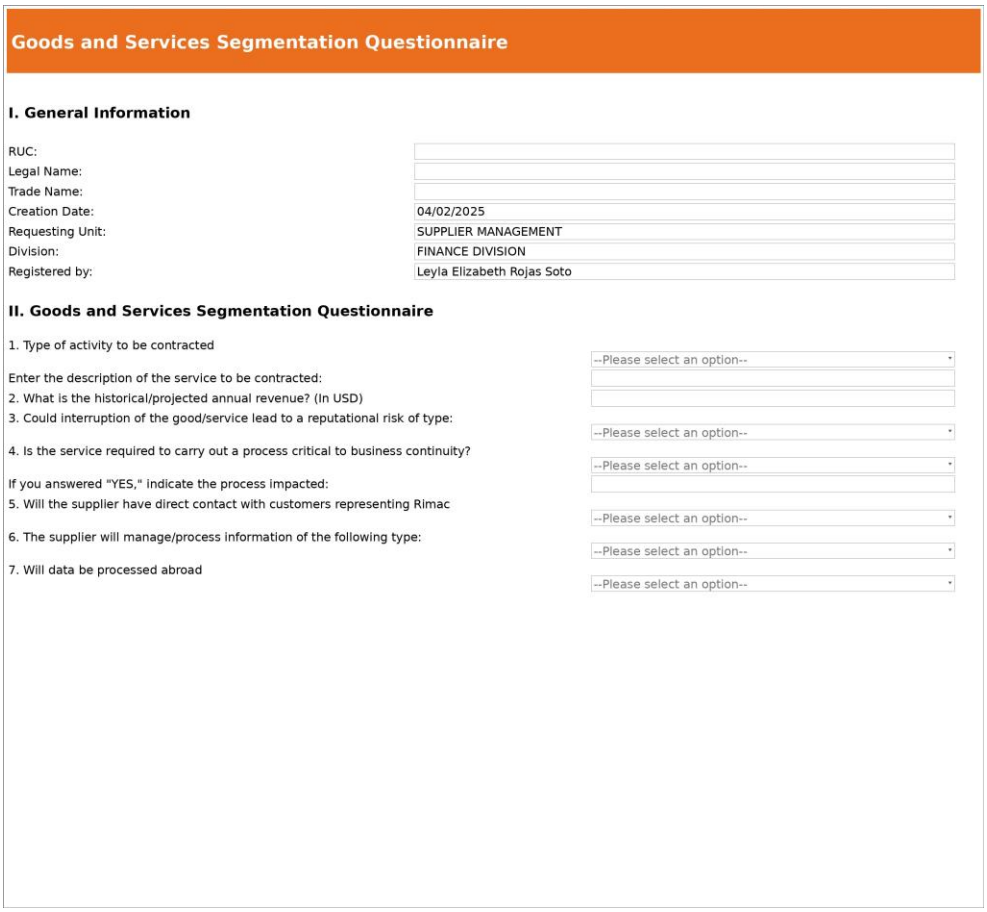
Due diligence corresponds to the requirements applied to the sourcing process. The strategy implemented must be aligned with the risk level established according to the rating of the product or service, as determined by the Risk area.

.

Due diligence consists of assessing whether a third party is suitable for establishing a business relationship with Rimac, taking into account financial, reputational and operational aspects. Once it is verified that the third party is suitable based on the product or service offered and the required risk assessments have been completed, those assessments make it possible to determine whether the controls implemented by the Third Party meet the standards set by Rimac.

7.1 Procurement Process Flow (Purchasing):

Note:
Regarding item 2, where it states (the full filter is performed), this activity means that the user must complete the supplier segmentation questionnaire and send an email to the Supplier Management mailbox (gestiondeproveedorescompras@rimac.com.pe) requesting registration of the supplier to be awarded the contract. Afterward, the Procurement area will send a link to the supplier's contact so they can complete the registration form by answering the following questionnaire for the segmentation of goods and/or services.mailto:gestiondeproveedorescompras@rimac.com.pe



Goods and Services Segmentation Questionnaire

I. General Information

RUC:	
Legal Name:	
Trade Name:	
Creation Date:	04/02/2025
Requesting Unit:	SUPPLIER MANAGEMENT
Division:	FINANCE DIVISION
Registered by:	Leyla Elizabeth Rojas Soto

II. Goods and Services Segmentation Questionnaire

1. Type of activity to be contracted	--Please select an option--
Enter the description of the service to be contracted:	
2. What is the historical/projected annual revenue? (In USD)	
3. Could interruption of the good/service lead to a reputational risk of type:	--Please select an option--
4. Is the service required to carry out a process critical to business continuity?	--Please select an option--
If you answered "YES," indicate the process impacted:	
5. Will the supplier have direct contact with customers representing Rimac	--Please select an option--
6. The supplier will manage/process information of the following type:	--Please select an option--
7. Will data be processed abroad	--Please select an option--

7.2 Due Diligence and Third-Party Risk Assessments

Due diligence is the process by which the potential risks associated with third parties and suppliers are identified and assessed; this procedure makes it possible to determine whether these suppliers can supply products and services to Rimac, considering their financial, operational, reputational characteristics and regulatory requirements. The exact approach for carrying out due diligence will vary according to the risk level associated with the purchase of the good or service.

For existing third parties, if the due diligence information is up to date and relevant to the acquisition, prior assessments should be leveraged to avoid duplicating effort.

Documentation related to third-party due diligence must be filed and kept in a record, safeguarded in a central repository in accordance with local procedures for purchases exceeding USD 80,000. The acquisition of products and services at Rimac shall respond to needs clearly identified by the requesting area.

It is essential that the Procurement area work together with the Risk area and the requesting business unit to design acquisition strategies and manage third-party risks, ensuring a secure approach for the company in sourcing products and services. Contracting must establish consistent processes with adequate controls, enabling business needs to be met through the most strategic and cost-effective method possible.

7.2.1 Requirements for Third-Party Due Diligence

The first step in the acquisition process is to specifically identify the business need regarding a good or service. If the contracting request is covered by the exceptions approved in the Procurement policy, the Procurement area does not need to intervene in the transaction. However, for all other contracting, rigorous due diligence must be carried out following the steps detailed below:

a. The user area must have an approved budget in order to proceed with the acquisition of the good or service.

b. The good or service to be contracted must first undergo the assessment of Goods and/or Services performed by the operational risk area.

c. The Procurement area will carry out the bidder tender process taking into account the recommendations issued by the Operational Risk area, based on the results obtained in the assessment of the good and/or service.

d. The user area must complete the Procurement area's segmentation questionnaire for the chosen supplier, in order to request the acquisition of the good or service and register the supplier.

e. If the good or service is considered critical and/or significant, a comprehensive risk assessment must be carried out.

f. The user area is responsible for responding to the requirements coming from the information security, crime prevention, technology risk, operational risk and business continuity areas, which constitute essential inputs for the risk assessment.

g. The Third Party's risk assessment must be submitted to the GIR committee, applicable for suppliers with significant contracting or subcontracting.

h. The residual risk obtained in the risk assessment will be the determining factor in establishing whether the Third Party is fit for contracting or whether control actions must be implemented for the acquisition of the good or service.

7.2.2 Budget and Approval

Every acquisition requested by the user area must have the corresponding budget approval.

Given this requirement and with the aim of optimizing time and resources, the requester from the user area must confirm budget availability prior to committing to the contracting process. In addition, if the relationship with the third party is expected to last more than one year, approval must be obtained from the executive vice-presidency of the user division for the entire duration of the relationship with the Third Party, before beginning due diligence and sourcing activities.

7.2.3 Consulting Services

Acquisitions related to consulting services must comply with the procedures set out in the third-party risk management policy. Consulting service engagements, regardless of the total amount to be spent, must have a budget or, failing that, must obtain approval from the executive vice-presidency of the user division and general management. Consulting services are not exempt from going through the goods and/or services assessment procedure (Phase 1); nor, where applicable, from the comprehensive risk assessment where required.

7.2.4 Price Due Diligence

Price due diligence consists of carrying out thorough research to establish an appropriate market value for the acquisition of a good or service. This process makes it possible to identify opportunities that ensure a fair negotiated price backed by solid grounds.

The Procurement area is responsible for carrying out due diligence in price assessment, implementing methods to determine fairness in pricing, under which it will assess the following aspects:

- Competitive bids
- Negotiated prices
- Comparison against industry benchmarks
- Comparison against historical prices

7.2.5 Development of the Sourcing Strategy

The sourcing strategy means that, if several third parties or suppliers are identified as qualified to provide the good or service, or if only a single third party is found suitable to meet a specific need, the requesting area and the Procurement team will seek to maximize purchasing power while mitigating risks through negotiated agreements with strategic third parties or through managed services, as applicable.

The sourcing process is led by the business requester, who assumes the same responsibilities as the Procurement area. When identifying possible third parties to meet a need, preference is given to existing suppliers under current contracts or current managed services programs.

Development of the sourcing strategy may take into account the following:

- Assessment of risks associated with the good or service
- Preparation of the budget
- Analysis of the supplier and its experience in the sector
- Comparison with other suppliers offering similar services
- Negotiation strategy
- Contractual components (SLA, KPIs, continuity plans, exit strategy, among others)
- Identification of key decision-making factors
- Third-party action and risk management plan, including criteria and documentary requirements for third-party management

7.2.6 Risk Assessment Exceptions (Pre-Contract)

In situations where user areas cannot wait for risk assessments to be completed before committing to a third party, a 60-day Exception Approval procedure may be used; this option should be used only in exceptional cases, such as market changes, regulatory requirements or specific demands from sole suppliers in the market.

.

Once the requester (user area) and the Procurement area decide to proceed with contracting the Third Party, the user area becomes responsible and is the main point of contact with the Third Party, as well as for communication with the Procurement area and Risk teams.

.

General management must approve exception requests, and the user area must document the justification for proceeding with the exception before the required risk assessments are finalized, and must provide an estimated time frame for their completion. It must also ensure follow-up on this date with the third party involved.

The Procurement, Legal and risk assessment teams, together with the user area, shall ensure that the necessary provisions are included in the contract signed with the third party. The process for approving 60-day exceptions is limited to certain specific risk assessments.

Risk Exception Escalation Matrix

The matrix describes the appropriate escalation levels according to the third party's inherent risk classification:

Extreme Risk	Proceeding is not permitted without carrying out the risk assessment
High Risk	Escalation to the General Manager + Risk EVP
Medium Risk	Risk EVP

Note: If a third-party company obtains an extreme inherent risk classification, exceptions cannot be granted under any circumstances.

Once the initial 60-day exception period has ended, the GIR Committee may authorize an extension of another 60 days.

8. CONTRACTS

Contracts are a formal document (with legal backing) under which the Third Party undertakes to transfer ownership of a good and/or provide a service to Rimac, and Rimac in turn undertakes to pay its price in money under the agreed terms and conditions.

Rimac must ensure that the contract with Third Parties specifies the following:

- Technical conditions and standards that the acquired goods and/or contracted services must meet,
- Service level agreements and applicable standards, at a technical level and at the level of our customers' (and stakeholders') experience,
- Operational details and guidelines.
- Key clauses to mitigate risks.
- Confidentiality and liability.
- Frequency of contract reviews.
- Contact details for monitoring satisfaction with the quality of the good or service and also for incident monitoring.
- Exit Strategy

9. FAST TRACK THIRD-PARTY EVALUATION

The Fast Track evaluation of Third Parties means that Third Parties must undergo a simplified evaluation, in which they will only go through Crime Prevention and Procurement Management review, in accordance with current procedures issued by these areas and the responsibilities described in the third-party risk management policy.

Fast track evaluations are carried out with the aim of reducing turnaround times and validating that the good or service is delivered on time and as agreed.
The Fast Track evaluation of Third Parties only applies to the following cases:

- Sole suppliers in the market
- Government entities
- Public utilities (water, energy, gas)
- Services with contracts of 30 days or less that are non-renewable, and with payment amounts for goods and/or services of S/ 15,000 or less

The FAST TRACK evaluation does not exempt the supplier from subsequently going through the Third-Party risk assessment (for regularization); this applies if the good or service provided by the third party is Critical and/or Significant.

10. DIRECT AWARD

Third Parties under direct award are those exempted from the requirement to submit more than one quotation when, due to the nature of the good or service, there is a sole supplier in the market, or when, even if several suppliers exist, only one of them can offer the minimum quality and safety conditions required by Rimac.

This also applies to the contracting of goods or services with Third Parties approved by the Management Committee, Emergency Committees on an urgent basis and/or the Board of Directors. Such approval must be recorded in the Committee/Board minutes.

Direct award contracting of S/. 15,000 or less:

- Supplier selection without the need for additional proposals.
- If the Logistics area (Procurement and Supplier Management) considers it necessary, it will apply this comparison approach for amounts below this threshold.
- This type of contracting must go through the Fast Track process.

Direct award contracting above S/. 15,000:

- Must be supported by a document justifying the choice of supplier, which must have the approvals described and mentioned earlier in this section, and must complete the Direct Award Form request.8
- This type of contracting must go through the corresponding third-party risk assessments.

Third Parties under direct award are not exempt from application of the third-party risk management policy and its methodology under Phase 1, and depending on the results, Phase 2 also applies.

DIRECT AWARD FORM

Supplier	
Amount	
Service and/or product:	
Mark the reason with an "X": 1. There is a sole supplier in the market. ☐ 2. Quotations were requested from other suppliers, but none were submitted. ☐ 3. There is more than one, the basis for the selection must be detailed in the corresponding field ☐	**If item 3 was marked, explain the reason for the selection:**

Requester	
Area	
Authorizing VP / EVP	

If, as a result of the risk assessment of a Third Party under Direct Award, observations arise regarding any of the risk fronts, the Third Party must remediate and implement, within no more than 3 months, the control actions requested by Rimac.

If the Third Party fails to implement the requested control actions within the agreed time frame, Rimac may proceed to terminate the contract through exit strategy clauses that must be included in the contract.

8 Annex 4 of the Administrative Procurement Management Policy

11. INCIDENT MANAGEMENT

Any incident related to third parties must be reported to the Risk division at: (riesgooperacional@rimac.com.pe). Likewise, upon detecting incidents related to third parties (non-compliance, data breaches, fraud, among others), the following must be done:mailto:riesgooperacional@rimac.com.pe

- Immediately notify the responsible area and the Risk division.
- Activate the process with the Third Party for identifying and escalating issues.
- Activate the incident management protocol according to severity and impact.
- Investigate the causes and define corrective and preventive actions.
- Communicate the results to senior management and, if necessary, to the regulatory authorities.
- An analysis, resolution and documentation process will be followed. Critical incidents will be escalated to the Comprehensive Risk Management Committee and remediation plans will be established.
- **The user area in charge of contracting the good or service is responsible for managing the incident with the Third Party (supplier) and complying with the guidelines described, and is also responsible for informing the Procurement and Risk areas of the actions taken for the corresponding follow-up and relevant control actions.**

12. EXIT STRATEGY

In the event of failure to implement action plans arising from the risk assessment, SLAs and other aspects that Rimac identifies regarding the Third Party, the contract must contain clauses for terminating the contractual relationship, and to that end the following guidelines must be implemented:

- A procedure must be in place for the safe and orderly termination of the relationship with third parties, under which the following will be carried out:
  - Assessment and/or satisfaction survey of the user area regarding the contracted good or service, evidencing any inconsistencies found.
  - Seek alternatives to replace the Third Party.
  - Establish strategies for the protection of information assets, return or destruction of sensitive information.
  - Have a schedule for settling outstanding obligations with the Third Party, and consider withholding payment if deliverables committed to Rimac are not met.
  - Strategies for transferring the services provided.
  - Assessment of the impact and communication to stakeholders.
  - Document the reasons for termination and analyze lessons learned to improve future contracting.

The Legal area is responsible for implementing the exit strategy for the contractual relationship with the Third Party.

13. UPDATE

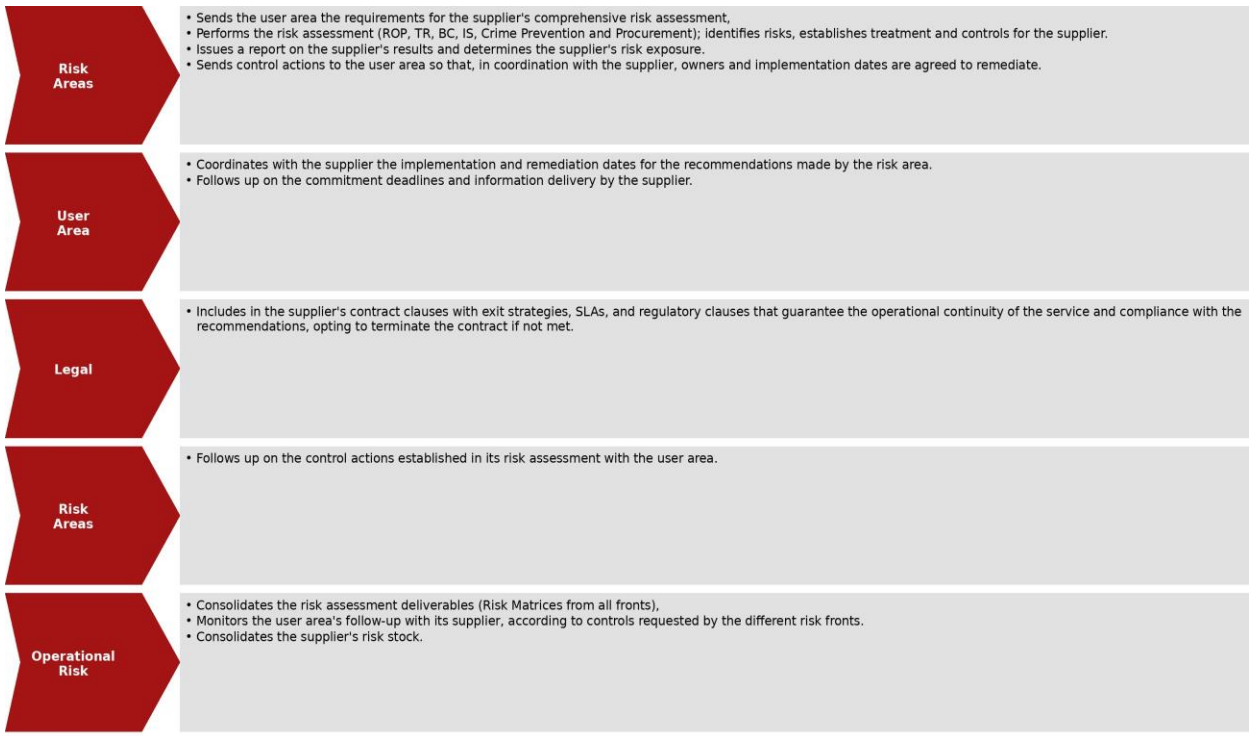
The risk assessment of a Third Party rated critical and/or significant must be updated every 2 years, if the contract remains in force; or upon a renewal.

14. OPERATING FLOW

This section shows the operating flow for gathering information for the risk assessment of goods and/or services – Phase 1 and for the supplier's risk assessment in Phase 2.

Phase I – Operating Flow - Assessment of Goods and/or Services

Phase II – Operating Flow - Supplier Risk Assessment



SLAs for handling Phase II risk assessments

1. Request for information submission by the user area, maximum time frame 2 weeks.
2. Delivery of the risk assessment by the areas involved, time frame 2 weeks.
3. Definition of dates and owners for action plans (agreements between the supplier and user area), time frame 1 week.

15. SUPPLIER REGISTRY DATABASE

Rimac must maintain a complete inventory of all its suppliers and third parties. The Procurement area is responsible for registering and updating the supplier inventory in coordination with the operational risk and legal areas.

The supplier inventory must have the following structure9:

Supplier Inventory Structure		
No.	**Fields**	**Description**
1	Service identifier	Unique code assigned by the company to identify the service; if none exists, use a sequential number
2	Service Name	Internal name used to identify the service received
3	Service Description	Description of the service received by the Company
4	Company Product/Service	Company product/service (user of the service)
5	Legal Name	Legal name of the supplier providing the service to the Company
6	Supplier's Tax ID (RUC)	Tax ID (RUC) of the supplier providing the service to the company
7	Location	Countries, regions and/or geographic areas from which the service is provided
8	Signature Date	Date the company and the supplier signed the start of the contractual relationship
9	Start Date	Start date of the service provision
10	Date of last renewal	Signature date of the last amendment to the contractual relationship between the company and the supplier.
11	End date	Expected date for the service provision to end.
12	Identification date	Date on which the methodology was applied to identify whether the service is significant or not.
13	Risk assessment date	Date on which the risk assessment was performed.
14	Supplier Rating	Indicates whether the service is significant or not.
15	Contracting Modality	Indicates whether the service is a subcontracting or direct contracting arrangement.

9 Supplier Inventory Structure / Official Letter No. 44461-2025-SBS - Annex 9.1: Third-party services currently in force (Ref.: 2025 Regular Inspection)

Supplier Inventory Structure		
No.	**Fields**	**Description**
16	Service Level Agreements	Indicates the number of service level agreements (SLAs) established for the provision of the service within the contract.
17	Exit Strategy	Indicates whether the contract has an exit strategy for the services provided by the supplier, allowing operations to resume in-house or through another supplier.

The Supplier Registry Database is updated monthly by the Procurement area for Rimac's new contracts, and annually for the renewal or contracting of significant services that remain in force.
Custody of the supplier registry database rests with the Operational Risk area.
The Supplier Registry Database is backed up monthly on the Risk division's SharePoint.

16. RELATED DOCUMENTS

< Internal or external documentation (regulations) related to the policy >.

CODE	NAME
POL-XXX	Third-Party Risk Management Policy
POL - 4540	Administrative Procurement Management Policy
POL - 4363	Administrative Supplier Management Policy
POL - 6061	Due Diligence Policy

17. ANNEXES

Not applicable

18. APPROVAL WORKFLOW OWNERS

Stage	Area	Position	Name
Preparation/ update	Risk	Operational Risk Manager	Melissa Tristan
Approval 1 (Content)	Risk	Operational Risk and Continuity Manager	Renato Bedoya
Approval 1 (Content)	Risk	Risk EVP	Ariel Roitman
Approval 2 (Content)	Procurement	Efficiency and Procurement Manager	Alberto Bardales

Stage	Area	Position	Name
Approval 2 (Content)	Legal	Legal Manager Advisory and Contracts	Rodolfo Grados
Operational Risk Approval /CGIR	Operational Risk Management	Operational Risk Manager	Renato Bedoya
Publication	Comprehensive Risk Management Committee /Board of Directors	Operational Risk and Business Continuity Manager	Renato Bedoya

(1) In the case of Rimac Seguros, the Market Conduct Officer will approve the Company's documents that relate to the management of market conduct within the organization, in accordance with the provisions of SBS Resolution 4143-2019 dated September 11, 2019, which approves the "Insurance System Market Conduct Management Regulation."

19. CHANGE CONTROL

Creation date or update	Description of the version	V	Author
09/15/2025	New Document	01	Melissa Tristan