RIMAC	**POLICY**				Code: POL-4881
	RISK MANAGEMENT IN AGILE ENVIRONMENTS				Version: 03
	Macro process:	Risk Management and Compliance	Process:	Operational Risk Management	Page 1 of 14

I. OBJECTIVE

Establish guidelines for preventive and corrective risk management in agile environments in the organization.

II. SCOPE

This policy applies to the Tribes deployed as part of the company's business agility model.

III. DEFINITIONS

- An event is an occurrence or sequence of events that might be internal or external to the company, originate from the same cause, and occur at the same time.

- New Product: A product launched for the first time by the company or a change in an existing product that significantly modifies its risk profile.

- Process: A set of organized and repeatable activities, tasks, and procedures that produce an expected result.

- Product: Goods and/or services provided by companies to their customers and users.

- Risk: the possibility of occurrence of events that negatively impact the company's objectives or its financial situation.

- Credit risk: The possibility of losses due to the inability or unwillingness of debtors, issuers, counterparties, or obligated third parties to meet their contractual obligations.

- Money laundering and terrorist financing risk: The possibility of the company being used for money laundering and terrorist financing purposes. This definition excludes reputational and operational risk.

- Liquidity risk: The possibility of losses from the early or forced sale of assets at unusual discounts to meet obligations, as well as the failure to close out open positions quickly or hedge positions in sufficient quantity and at a reasonable price.

- Market risk: The possibility of losses arising from fluctuations in interest rates, exchange rates, prices of equity instruments, and other market prices, which affect the valuation of positions in financial instruments.

- Reputational risk: The possibility of losses from diminished confidence in the integrity of the institution that arises when the good name of the company is affected. Reputational risk may arise from other risks inherent in an organization's activities.

- Strategic Risk: The possibility of losses due to high-level decisions associated with the creation of sustainable competitive advantages. It is related to failures or weaknesses in the analysis of the market, trends, and uncertainty of the environment, key competencies of the company, and in the process of value generation and innovation.

- Operational Risk: The possibility of losses due to inadequate processes, personnel failures, information technology failures, or external events. This definition includes legal risk but excludes strategic and reputational risk.

- Technical Risk: The possibility of loss or adverse change in the value of commitments under insurance, reinsurance, and coinsurance contracts. In the case of non-life insurance, fluctuations related to the frequency, severity, and settlement of claims are considered. For life insurance, this may include the possibility of losses due to variations in the level, trend, or volatility of mortality, longevity, disability, morbidity, renewal, or surrender rates of insurance contracts, among other parameters and assumptions, as well as the expenses of executing such obligations.

- Reinsurance risk: The possibility of losses in the event of insufficiency of the reinsurance coverage contracted by the ceding insurance company, when the reinsurance needs were not identified, determined or adequately specified in the contracts; or when the reinsurer is not able to meet its payment commitments or is not willing to pay them due to discrepancies in the application of the conditions of the insurance and/or reinsurance contract; as well as the delay in the reinsurer's payments that may affect the ceding company's cash flows, generating a liquidity risk. In accepted reinsurance, it includes the risk derived from the application of an inadequate rate by the ceding company and the risk of suffering the same fate, for which as reinsurer it will participate in the results, positive or negative, to which its ceding company is exposed by virtue of direct insurance.

- Risk Wall: It is the artifact that allows the identification and centralization of risks in the Tribe.

- Risk Marketplace: It is the event that allows sharing and disseminating the findings at the level of risks and mitigation measures of the tribe.

- Subcontracting: Management modality by means of which a company hires a third party to develop a process that could be carried out by the contracting company.

- Significant Subcontracting: Subcontracting that, in the event of service failure or suspension, could put the company at significant risk by affecting its income, solvency, or operational continuity.

IV. RESPONSIBILITIES

4.1. Tribe

Tribe Leader

- Ensure that risks are assessed by applying the methodologies defined by each Risk unit.
- Allocate the necessary resources to manage the main risks identified.
- Develop a risk management culture in the Tribes.
- Identify and manage risks associated with the processes and products managed in the Tribe.
- Ensure that inherent risks are regularly assessed.
- Implement mitigation measures for the main risks identified.
- Validate that the controls in place are effective.
- Ensure the management of loss events generated in the Tribe.
- Ensure systematic and consistent application of the Risk & Control model throughout the Tribe.
- Implement the Information Security controls defined in the design of the initiative.

Safe Business Officer

- Ensure that a strategic view of risk management is in place.
- Promote risk management culture in the Tribe.
- Identify risks with common causes in the Tribe.
- Identify cross-cutting action plans/improvement opportunities.
- Ensure consistency of Tribe Risk Base (cause - event - consequence).
- Prioritize the treatment of risks with the Tribe leader.
- Ensure that the Risk Wall is strengthened and kept up to date.
- Coordinate and present information in Risk Marketplace.
- Managing risks where there is interdependence in other Tribes
- Interact with other SBOs to synchronize common responsibilities and coordinate joint attention to companies' requirements.
- To be the channel for queries and requirements of the risk areas.
- Coordinate and present the status update on the implementation of standards.
- Promote compliance with annual campaigns (Regulatory Courses, Conflicts of Interest, and Sworn Statement of Assets).
- Manage action plans for the Tribe's major risks and losses.

Product Owner / SMT Leader

- Examine the environment in which it develops its processes.
- Identify, analyze, and assess the risks associated with the processes and products managed in his/her squad / SMT.
- Managing the sources of risk and providing timely treatment.
- Implement mitigation measures for the main risks identified.
- Ensure that the controls in place are effective.
- Identify operational risk events materializing in losses for the Tribe.
- Provide support to the Safe Business Officer in the strengthening of the Risk Wall and its dissemination in the Risk Marketplace.
- Ensure systematic and consistent application of the Risk & Control model in his/her squad / SMT.

4.2. Legal and Regulatory Division

Regulatory Compliance

- Ensure proper compliance with the regulations applicable to the Company, both internal and external.
- Ensure the proper functioning of the Anti-Corruption Management System, establishing policies, procedures, and controls to prevent, detect and manage criminal and reputational risks, among others, that may expose the company; mainly, ensuring compliance with the Anti-Corruption Policy.

Prevention of Money Laundering and Financing of Terrorism

- Control the risk of third parties using Rimac Seguros y Reaseguros (RIMAC) as a means to launder assets and/or finance terrorism.
- Monitor compliance with the Money Laundering and Terrorism Financing Prevention System (LAFT) based on SBS Regulation No. 2660-2015, Law No. 27693, Law that creates the Financial Intelligence Unit of Peru - UIF-Peru and other regulations in force issued by the Superintendency of Banking, Insurance and Pension Funds (SBS).

Legal Counsel

- To provide legal advice to ensure that the contracts entered into and the documents issued comply with the legal provisions in force.
- To resolve legal and regulatory consultations formulated by other areas of Rimac.

Contentious Proceedings

- Prevent, avoid, and/or mitigate all legal contingencies that could derive or derive from administrative, judicial, or arbitration processes of the company at the national level.
- Provide advice in the company's defense and coordination with external firms.

4.3. Finance and Risk Control Division

Actuarial

- Ensure that new products or modifications to current products have correct technical pricing and that this is known to the Tribes and is reflected in the Technical Note.
- Communicate in a timely manner the information needs for the calculation of reserves and technical pricing.
- Include changes in conditions and new products for the calculation of technical reserves.
- Evidencing the accounting impact of reserves as part of the considerations to be taken into account by the business for the launching of new products.
- Monitor and diagnose the profitability of existing products, generating insights for the prioritization of tasks in the Tribes.

Business Continuity

- Propose policies, procedures, and methodology for business continuity management in the company, assigning roles and responsibilities, and establishing alignments to ensure proper business continuity management.
- Ensure competent, effective business continuity management that is integrated into the company's organizational culture.
- Inform the General Management and the Integral Risk Management Committee about relevant aspects of business continuity, for timely decision making.

Technical Risks

- Define and maintain the company's technical risk policy, as well as verify its compliance.

- Define and develop methodologies for the identification and evaluation of technical insurance risks in accordance with the provisions of the Board of Directors and the Comprehensive Risk Management Committee.
- Ensure compliance with all regulations related to the management and/or control of technical insurance risks.
- Raise awareness of the Tribes in the identification and assessment of technical insurance risks.
- Evaluate the technical risks associated with the launch of new products or major modifications to the characteristics of existing products.
- Communicate to the Integrated Risk Management Committee, general management, and/or technical operating areas about the main technical insurance risks to which the company is exposed or could be exposed, and suggest mitigation plans.
- Report to regulatory agencies regarding the management of technical risks, as established in the current regulatory framework.

Operational Risks

- Propose the organization's operational risk management policies, as well as verify compliance with them.
- Implement and deploy operational risk management methodologies in accordance with the provisions of the Board of Directors and the Comprehensive Risk Management Committee.
- Training the Tribes in risk management.
- Assist Tribes in the management and assessment of operational risks in the Tribe.
- Report to the Comprehensive Risk Management Committee and the Board of Directors the results of management and the main exposures assumed.
- Report to Regulatory Bodies regarding the management of operational risks, as established in the current regulatory framework.
- Ensure the implementation of operational risk dashboards in the Tribes.
- Ensure a record of the Tribe's operational risk losses.
- Evaluate the risks associated with new product launches or the implementation of major changes in the business, operational, and IT environment.
- Propose the implementation of action plans for the main operational risks and ensure their implementation within the defined timeframes.

Fraud Prevention

- Assist Tribes in Fraud Prevention in the face of new product launches or the implementation of major changes in the business, operational, and IT environment.
- Propose actions to mitigate the risk of fraud.
- Follow up on research plans.
- Maintain Rimac's Fraud Prevention Policy.
- Maintain a record of fraud events that occur in the company.
- Carry out fraud event investigation plans, involving the necessary areas and employees.

Technology Division

Information Security

- Define Information Security guidelines and disseminate them for compliance.
- Review the context of the projects and based on the evaluation define the information security risk profile in the different initiatives of the tribal squads in order to carry out the respective analysis and evaluation based on the Information Security risk manual.
- Perform compliance checks.
- Manage the closure of proposed mitigation actions.

V. DEVELOPMENT

V.1 Implementation of Risk & Control model

An agile organization provides an opportunity to strengthen the scope of the three lines of defense model and improve the speed of 2nd line responses. The risk management system seeks to implement a decentralized model, called Risk & Control. The risk management model deployed in the Tribes is aligned with non-financial risk management models, in particular operational risk management.

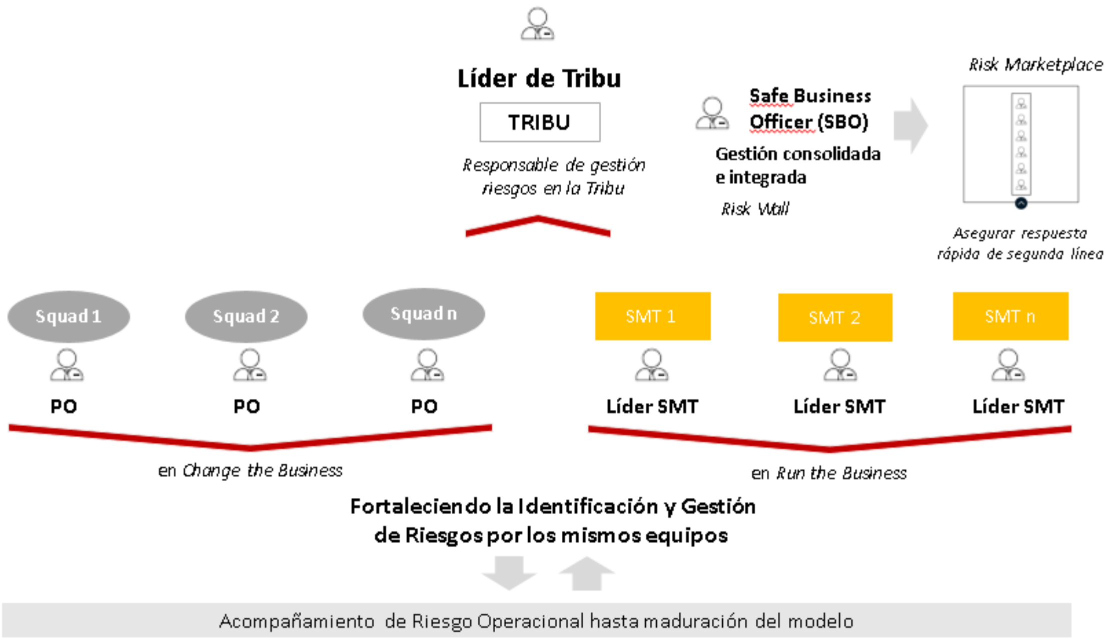
The model seeks to ensure risk management in the following stages:

- *Change the Business*: Reducing the risk of initiatives implemented by Squads.
- *Run the Business*: Maintaining a controlled risk profile in SMTs.

Likewise, the model seeks to achieve:

- Increase risk management culture in Squads and SMTs Initiatives.
- Ensure visibility of Tribe's risks for risk management (Risk Wall and Risk Marketplace).
- Reducing the impact of risks and losses within the Tribes.
- Reduce 2nd line response time.

The proposed decentralization model is based on strengthening risk identification and management from the Squads and SMTs, with the support of the operational risk team. Additionally, the model is supported by the role of the Safe Business Officer, who consolidates and integrates the Tribe's risk information in order to coordinate the treatment measures with the Tribe Leader, who is ultimately responsible for risk management. The following chart shows the Risk & Control model decentralization proposal.



Líder de Tribu
TRIBU
Responsable de gestión riesgos en la Tribu
Safe Business Officer (SBO)
Gestión consolidada e integrada
Risk Wall
Risk Marketplace
Asegurar respuesta rápida de segunda línea
Squad 1
Squad 2
Squad n
PO
PO
PO
SMT 1
SMT 2
SMT n
Líder SMT
Líder SMT
Líder SMT
en Change the Business
en Run the Business
Fortaleciendo la Identificación y Gestión de Riesgos por los mismos equipos
Acompañamiento de Riesgo Operacional hasta maduración del modelo

The operational risks team provides support during the maturity stage through the role of a risk expert, who is responsible for:

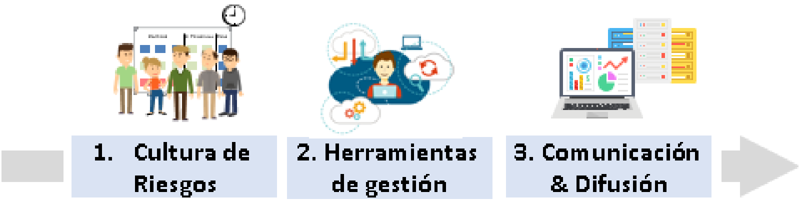
- Fostering a risk management culture in the Tribe.

- Ensuring the adoption of the model.
- Validating that risks are quantified (value capture).
- Deploying methodological guidelines.
- Proposing new risks with information from Tribe events (Review, PO Sync, etc).
- Ensuring validation of Risk Wall by SBO and Tribe leader.

The Risk & Control model promotes the continuous measurement of the tribe's risk profile, the incorporation of corrective actions in the backlog, and the formal treatment of identified risks. The key success factors of the model are:

- Generate Value: Ensure it matters to the first line of defense.
- Achieve Maturity: Ensure understanding of risk management in all businesses.
- Ensure Adoption: Make it part of the Tribe's recurring activities.
- Designate resources: Promote team dedication.
- Fostering Culture: Continued strengthening throughout the Tribe.

The implementation cycle of the Risk & Control model consists of three stages, which are shown in the following chart:



V.1.1 Risk management culture

The first stage of the Risk & Control model implementation cycle consists of fostering the risk management culture in the Tribes. This stage aims at ensuring that the model is integrated into the operations of the first line of defense, being a key continuous process to ensure the maturity of the model.

The operational risk team holds sessions to disseminate the importance of risk management, share case studies, and present the methodology for the management model, from identification, declaration, and treatment of risks. Proposals for the development of tools, artifacts, and events are also reviewed. The topics discussed and disseminated in the culture sessions are as follows:

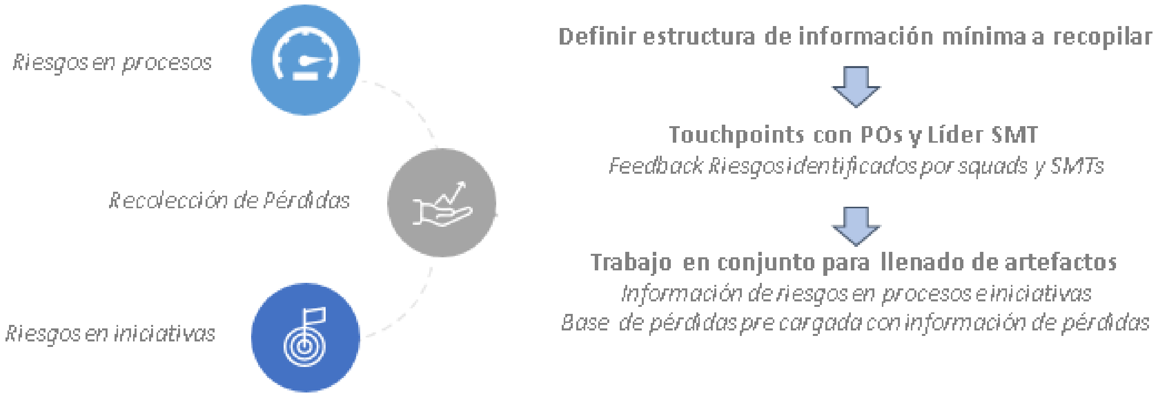
Sesión 1	Sesión 2	Sesión 3
La importancia de la Gestión de Riesgos	¿Cómo identificar y declarar los riesgos?	¿Cómo crear el Risk Wall de la Tribu? Risk Marketplace

Tribe Leaders, Technical Leaders (TTL), and Agile Coaches (AC), Product Owners (PO), SMT Leaders, and Safe Business Officers (SBO) are all invited to these sessions. The first session addresses the importance of risk management and how it generates value in tribes. The second session promotes a practical theoretical approach to risk identification and assessment. The third session aims to establish the guidelines for the development of the risk identification artifact (Risk Wall) and the design of the management dissemination event (Risk Marketplace).

V.1.2 Management tools

In the second stage of the Risk & Control model implementation cycle, tools are provided for risk identification and consolidation. This stage aims to ensure that the risks of the tribes are identified, the exposure to risks is measured and treatment measures are defined.

The operational risk team has developed tools and forms for risk identification and management. These are a first version that will be enriched through iterations in this process. Risk identification is at the level of processes, initiatives, and loss materialization.



Definir estructura de información mínima a recopilar

Touchpoints con POs y Líder SMT
Feedback Riesgos identificados por squads y SMTs

Trabajo en conjunto para llenado de artefactos
Información de riesgos en procesos e iniciativas
Base de pérdidas pre cargada con información de pérdidas

In the first stage, the development of tools is worked on jointly by the operational risk team and the tribe as part of the model maturity process.

For the development of management tools, it is necessary to have different views on risks in order to enrich the analysis. For this stage of the cycle, interaction and alignment between the business and control areas is key.

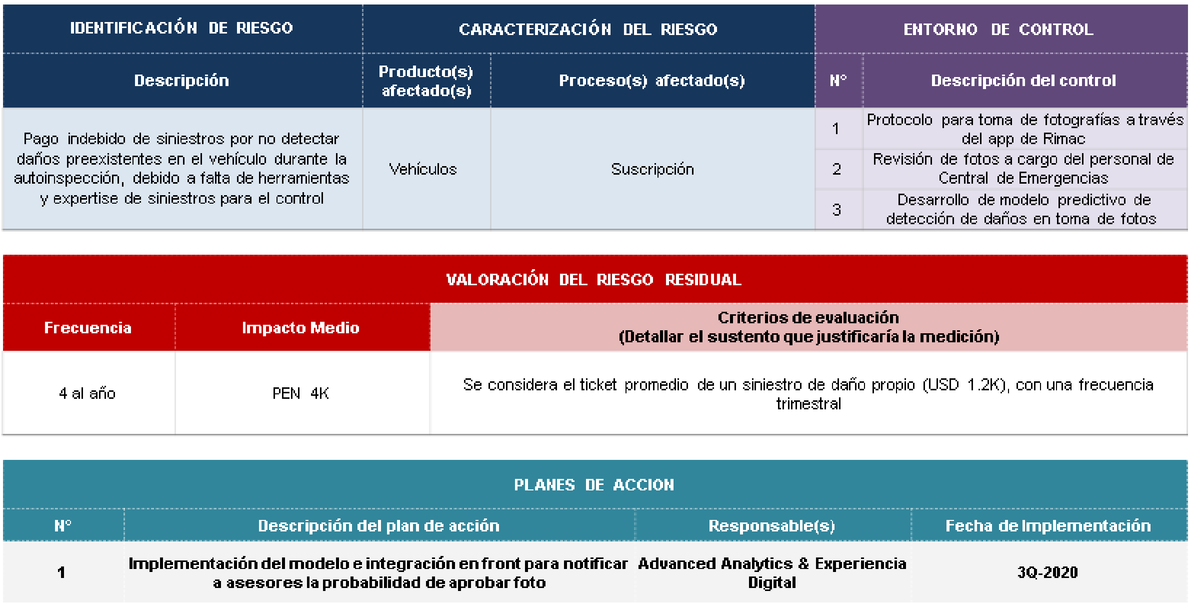
Touchpoints are held with each Squad and SMT to ensure deployment of the methodology and to provide feedback on identified risks.

The tribe leader is responsible for ensuring that these risk management tools and artifacts are incorporated into the recurring work of the Tribes in order to ensure the adoption of the decentralized risk management model. Likewise, the second line of defense teams participate in the tribe's own events to learn about initiatives and results that allow them to identify new risks (Big Room Demo, Big Room Planning, Reviews, etc.).

As a minimum structure of the risk base, the following fields have been defined:

1. Identification of risks, detailing causes, events, and consequences of the risk. The risk and the control environment are characterized.
2. Residual risk assessment, considering the impact and residual frequency of the risk in order to determine its exposure.
3. Action plans, detailing risk mitigation measures, considering the date of implementation.

The following tables provide an example of the risk basis structure:



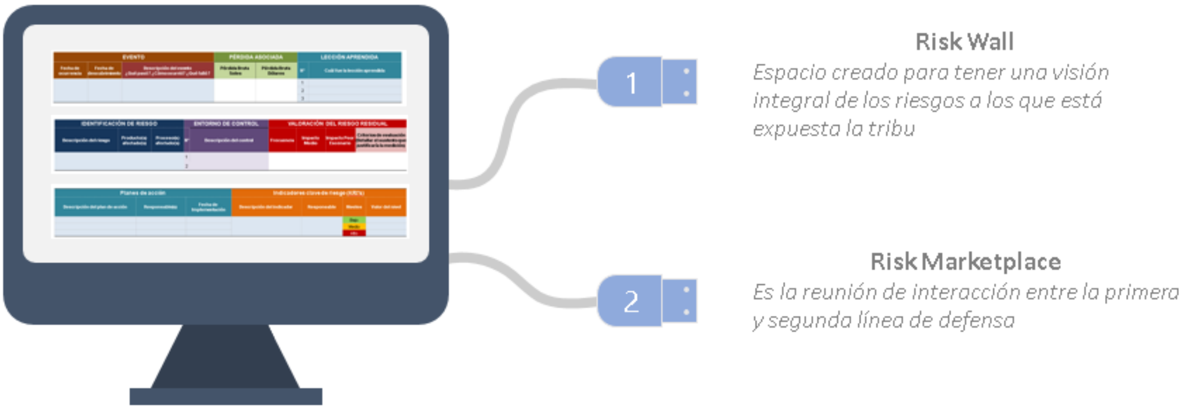
IDENTIFICACIÓN DE RIESGO	CARACTERIZACIÓN DEL RIESGO		ENTORNO DE CONTROL	
Descripción	Producto(s) afectado(s)	Proceso(s) afectado(s)	N°	Descripción del control
Pago indebido de siniestros por no detectar daños preexistentes en el vehículo durante la autoinspección, debido a falta de herramientas y expertise de siniestros para el control	Vehículos	Suscripción	1	Protocolo para toma de fotografías a través del app de Rimac
			2	Revisión de fotos a cargo del personal de Central de Emergencias
			3	Desarrollo de modelo predictivo de detección de daños en toma de fotos

VALORACIÓN DEL RIESGO RESIDUAL		
Frecuencia	Impacto Medio	Criterios de evaluación (Detallar el sustento que justificaría la medición)
4 al año	PEN 4K	Se considera el ticket promedio de un siniestro de daño propio (USD 1.2K), con una frecuencia trimestral

PLANES DE ACCION			
N°	Descripción del plan de acción	Responsable(s)	Fecha de Implementación
1	Implementación del modelo e integración en front para notificar a asesores la probabilidad de aprobar foto	Advanced Analytics & Experiencia Digital	3Q-2020

V.1.3 Communication and Dissemination

In the third stage of the implementation cycle of the Risk & Control model, the communication and dissemination of risks and their treatment is promoted. This stage includes a Risk Wall and a Risk Marketplace.


1
Risk Wall
Espacio creado para tener una visión integral de los riesgos a los que está expuesta la tribu
2
Risk Marketplace
Es la reunión de interacción entre la primera y segunda línea de defensa

The Risk Wall (artifact generated from the risk base) is the physical or virtual space created to have a comprehensive view of the risks to which the tribe is exposed. This artifact is intended to promote the discussion of risks, lessons learned, and mitigation measures (Bottom-Up), as well as to serve as a repository of mitigation plans pending implementation (Backlog). This artifact is generated by the Safe Business Officer and validated by the Tribe Leader.

The Risk Marketplace (event) is the physical or virtual meeting between the first and second line of defense convened by the Tribe, where the main risk exposures identified are discussed, as well as the treatment of the risks that have been declared on the Risk Wall. The objectives of this event are to:

- be the means for discussion and analysis of risks.

- analyze specific risks.
- include relevant unidentified risks.
- agree on the response to risks and specific actions to mitigate them.
- prioritize action plans in Tribe's backlog.

V.2 Operational Risk Management

The operational risk management system involves the development of objectives, policies, procedures, and actions in order to identify, measure, control, and disclose the risks to which the Company is exposed by each unit responsible for processes and products. The operational risk management model deployed in the Tribe is aligned with (1) the management model developed by Rimac Seguros, as detailed in the Operational Risk Manual, and (2) current regulations.

The operational risk management seeks the following objectives:

- Promote a risk management culture that allows the development of a balance with commercial policies.
- Develop tools that allow the timely identification, measurement, and control of operational risk.
- Ensure a communication and dissemination mechanism that allows for efficient operational risk management.

The operational risk management deployed in the company comprises the following management elements, all framed within the methodological framework detailed in the policies and procedures of Rimac Seguros' Operational Risk Management Manual.

The Company's operational risk management is supported by the following principles:

- Effective risk management provides greater assurance regarding the achievement of the company's vision and objectives.
- Each Tribe is expressly responsible for managing the operational risks associated with its business objectives.
- All significant risks shall be identified, assessed, mitigated, monitored, and reported by the Tribe leader.

Operational risk management mainly comprises the following activities:

Awareness

Awareness is a key component in identifying and taking appropriate actions to mitigate risks. Ongoing staff training and adequate disclosure of the threats to which the main processes are exposed are essential components of risk mitigation measures.

The Operational Risk Unit, with the cooperation of Tribal leadership, will apply the following principles with respect to communication/disclosure of information and training of personnel:

- Promote awareness of the operational risks faced by the Tribe.
- Ensure the availability of personnel with the necessary competencies for operational risk management.
- Provide training to personnel to create the necessary competencies for the solution of problems related to operational risk management.

Evaluation

The evaluation of operational risks is based on the identification of internal and external threats to which the main processes are exposed and which may have a negative impact on the Company's objectives, considering the influencing factors that determine them. Likewise, the impact of these threats is determined, and the subsequent evaluation of the controls is implemented to mitigate the risks associated with these threats.

Tribe Leaders must ensure that:

- Operational risks are assessed by applying the methodology formally defined by the Operational Risk Unit.

- The risks inherent to the functions and processes under its responsibility are adequately mitigated and regularly evaluated.
- The financial cost of mitigation measures is appropriate in terms of the cost or financial loss of the materialized threat.
- The controls in place are operating effectively.
- Controls are in place to assess the risks associated with changes in operations (new products, new projects, changes to systems in use, etc.).
- The scope of the operational risk assessment processes covers not only the internal environment but also the external environment.

Mitigation

Operational risk management is an ongoing process and Tribe leaders must ensure that risks are reviewed on a regular basis and that appropriate mitigation measures are implemented.

Risk Treatment

It involves the process through which the risk is accepted, the probability of occurrence is reduced, the impact is lessened, the risk is totally or partially transferred, it is avoided, or a combination of the above measures.

Tribe Leaders should ensure that periodically the following is performed:

- Review of the effectiveness of the implemented mitigation measures.
- Ensure that the information contained in the reports is effectively used to formulate and take appropriate actions.
- Evaluate the measures implemented to reduce the Company's exposure to operational risks.

The Operational Risk Unit shall provide support to management to fulfill these responsibilities.

Monitoring and Reporting

Monitoring and reporting are critical to ensure that the operational risk management process is efficient in the organization.

At the strategic level: The Operational Risk Unit shall inform the Board of Directors and General Management in a timely manner of any development or initiative in the organizational strategy that could have significant effects on the risks associated with the Tribe's operations.

At the operational level: the Operational Risk Unit shall be informed in a timely manner by the Tribe Leaders of the following:

- Proposals for new operating procedures, systems, or business models to be implemented.
- Evidence or suspicion of internal fraud and dishonesty of Tribal members.
- Launch of new products or modifications to existing products
- Hiring or subcontracting providers in the Tribe's processes.
- The main operational risk losses that have materialized in the Tribe.

VI. ANNEXES

Not applicable

VII. RELATED DOCUMENTS

CODE	NAME
MAN - 4382	Operational Risk Management Manual

VIII. PERSONS RESPONSIBLE FOR THE APPROVAL FLOW

Stage	Area	Cargo	Name
Elaboration/ update	Operational Risk	Assistant Manager of Operational Risks	Carlos Higa
Approval 1 and 2 (Contents)	Risks	Vice President	Silvana Sarabia
Market Conduct Officer Approval	Market Conduct Officer (1)	Market Conduct Officer	Elio Bernos
Approval (Methodology)	Business Process Engineer	Business Process Engineering **ROLE:** Documentary Management Administrator	Angelka Machay
Operational Risk Approval /CGIR	Operational Risk Management	Assistant Manager of Operational Risks	Carlos Higa
Publication	Integral Risk Management Committee / Board of Directors	Assistant Manager of Operational Risks	Carlos Higa
Publication Management	Business Process Engineer	Business Process Engineer	Angelka Machay

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

IX. CHANGE CONTROL

DOCUMENT CREATION			
DATE OF PREPARATION	**DESCRIPTION**	**V**	**AUTHOR**
06/23/2020	Risk Management Policy in Agile Environments	01	Edson Rojas

DOCUMENT UPDATE RECORD

REPLACES PUBLISHED DOCUMENT		DESCRIPTION OF THE UPDATE	V	AUTHOR / UPDATER
DATE OF PUBLICATION	CODE	Comprehensive review and update of the document.	02	Carlos Higa
07/01/2020	POL -3987			
DATE OF PUBLICATION	CODE	Update on risk management responsibilities in agile environments at the Tribe member level.	03	Carlos Higa
06/23/2021	POL - 4392			