



7

Gestión de Riesgos Risk Management

7.1. Gestión de riesgos
7.1. Risk management

Gestión de riesgos

Árma considera la gestión de riesgos de especial relevancia dentro del área de gobierno corporativo, ya que se encuentra sujeta a un amplio espectro normativo y de buenas prácticas en materia de cumplimiento y *reporting*. Para dar respuesta a estos requerimientos, Árma ha implementado un Modelo de Gestión de Riesgos que se basa en:

- ▶ Sistema de Gestión de riesgos (SGR - Cumplimiento, Entorno, Sostenibilidad, Estratégico, Financiero y Operativo).
- ▶ Modelo de Prevención y Detección de Delitos (MPDD).
- ▶ Sistema de Control Interno de la Información Financiera (SCIIF).

Con el fin de:

- ▶ Dar cumplimiento a la normativa aplicable.
- ▶ Contar con unos modelos adaptados a las características de Árma.
- ▶ Dar confort en la toma de decisiones interna y a terceros a través del *reporting* de estos ámbitos.

El Consejo de Administración considera la gestión de los riesgos y el control interno factores esenciales para la consecución de los objetivos de la Sociedad. Para su aplicación, cuenta con la colaboración de la Comisión de Auditoría y Control la cual, a su vez, se apoya en la Función de control y gestión de riesgos. En este contexto, Árma cuenta con un Modelo de Gestión de Riesgos que tiene su base en la Política de Control y Gestión de Riesgos, la cual se desarrolla en el Manual de Control y Gestión de Riesgos. Este Modelo incluye, en línea con su compromiso de integrar la sostenibilidad en todos los niveles de la empresa, un análisis de riesgos *ESG* (*Environmental, Social, Governance*).

La Compañía lleva a cabo un procedimiento sistemático y preventivo, alineado con los estándares internacionales de referencia en materia de gestión de riesgos (COSO¹ ERM 2017 - Marco de gestión de riesgos empresariales) y liderado por la Dirección, con el fin de abordar los riesgos mediante la previsión, la prevención y la detección de los mismos.

La gestión y control de riesgos es un proceso continuo que se fundamenta en (i) la identificación y evaluación de los potenciales riesgos de la Compañía a partir de los objetivos estratégicos y de negocio, (ii) la determinación de los planes de acción y controles de los riesgos críticos, (iii) la supervisión de la eficacia de los controles diseñados y de la evolución del riesgo residual para su reporte a los órganos de gobierno de la compañía.

Asimismo, el Sistema de Gestión de Riesgos funciona de forma integral, continua y transversal, y atiende a la gestión de todos los riesgos prioritarios, tanto internos como externos.



Una vez identificados los riesgos que pueden afectar a la consecución de los objetivos de la Compañía, son evaluados desde una doble perspectiva: probabilidad de ocurrencia e impacto (valoración del riesgo residual). Posteriormente, se evalúa el nivel de control sobre los mismos y, por último, son representados gráficamente en un Mapa de Riesgos corporativo.

El marco regulatorio español en materia de control interno establece distintas obligaciones para las sociedades cotizadas, entre las que se encuentra hacer público con carácter anual un Informe de Gobierno Corporativo. En este documento se deben incluir, entre otros aspectos, una descripción de las principales características de los sistemas internos de control y de gestión de riesgos en relación con el proceso de emisión de la información financiera.

(1) El "Committee of Sponsoring Organizations" (COSO) es una organización voluntaria del sector privado fundada en 1985 cuya misión es proporcionar liderazgo intelectual en relación a tres temas interrelacionados: la gestión del riesgo corporativo, el control interno y la disuasión del fraude.

Risk management

Árma considers risk management of special relevance within the area of corporate governance, as it is subject to a wide range of regulations and best practices in compliance and reporting. In order to respond to these requirements, Árma has implemented a Risk Management Model based on:

- ▶ Risk Management System (RMS – Compliance, Environment, Sustainability, Strategic, Financial and Operational)
- ▶ Crime Prevention and Detection Model (CPDM)
- ▶ Internal Control over Financial Reporting System (ICFRS)

In order to:

- ▶ Comply with applicable regulations.
- ▶ Benefit from models adapted to Árma's specific characteristics.
- ▶ Aid decision-making internally and with third parties through the reporting of these areas.

The Board of Directors considers risk management and internal control to be essential factors for the achievement of the Company's objectives. In order to implement these measures, the Company benefits from an Audit and Control Committee which, in turn, relies on the Risk Control and Management Function. Árma has therefore established a Risk Management Model based on the Risk Management and Control Policy, which is detailed in the Risk Management and Control Manual. This Management model includes, in line with its commitment to integrate sustainability at all levels of the Company, an ESG (*Environmental, Social, Governance*) risk analysis.

The Company carries out a systematic and preventive procedures, aligned with renowned international risk management standards (COSO¹ ERM 2017 - Enterprise Risk Management Framework) and led by Management, in order to address risks by anticipating, preventing and detecting them.

Risk management and control is a continuous process based on (i) the identification and assessment of potential Company risks based on strategic and business objectives, (ii) the determination of action plans and controls for critical risks, (iii) monitoring the effectiveness of the controls and residual risk developments put in place, to report to the Company's governing bodies.

(1) The "Committee of Sponsoring Organizations" (COSO) is a voluntary private sector organization founded in 1985 whose mission is to provide intellectual leadership in relation to three interrelated issues: corporate risk management, internal control and fraud deterrence.

In addition, the Risk Management System operates in a comprehensive, continuous and cross-cutting way, and serves the management of all priority risks, both internal and external.



Once the risks which may affect the achievement of the Company's objectives have been identified, they are assessed from a dual perspective: probability of occurrence and impact (residual risk assessment). Subsequently, the level of control over them is evaluated and, lastly, they are graphically represented on a Corporate Risk Map.

The Spanish regulatory framework on internal control establishes various obligations for listed companies, including the publication of an Annual Corporate Governance Report. This document must include, among other aspects, a description of the main characteristics of the internal control and risk management systems in relation to the process of issuing financial information.

Con el objetivo de dar cumplimiento a los requisitos legales y alinearse con las buenas prácticas del mercado, Árima cuenta con:

- ▶ Una Comisión de Auditoría y Control para efectuar, entre otras funciones, la supervisión de la eficacia de los sistemas de control y gestión de riesgos y de los procesos de elaboración y presentación de la información financiera de la Sociedad⁽²⁾.
- ▶ Un Sistema de Control Interno de la Información Financiera (SCIIF) que ayuda a proporcionar una seguridad razonable sobre la fiabilidad de la información financiera que facilita Árima a sus grupos relevantes, tanto externos como internos, respecto los procesos clave, operativos y no operativos, con impacto significativo en la información financiera y en la prevención del fraude.

El procedimiento de gestión de riesgos sobre la información financiera de Árima cuenta con los siguientes pilares:

Objetivos: determinan el ámbito de actuación del Sistema de Control Interno de a Información Financiera implantado.

Entorno de control: define la organización y las responsabilidades de los diferentes intervinientes en relación al SCIIF.

Metodología del Sistema de Control Interno de la Información Financiera: define las actividades, prácticas, procedimientos y herramientas técnicas facilitadas para el correcto desarrollo del Sistema de Control Interno de la Información Financiera implantado. En este sentido, el Proceso de SCIIF consta de las siguientes partes fundamentales:



Identificación y evaluación de riesgos



Determinación y documentación de procesos y controles clave



Monitorización y Reporting



Actualización del SCIIF



(2) Artículo 35 del Reglamento del Consejo de Administración de la Sociedad.

In order to comply with legal requirements and align with best market practices, Árima has:

- ▶ An Audit and Control Committee to, among other functions, supervise the effectiveness of the control and risk management systems and of the processes of preparation and presentation of the Company's financial information⁽²⁾.
- ▶ An Internal Control over Financial Reporting System that helps to provide reasonable assurance on the reliability of the financial information provided by Árima to its relevant external and internal stakeholders with respect to key operational and non-operational processes with a significant impact on financial reporting and fraud prevention.

Árima's financial information risk management procedure has the following pillars:

Objectives: determine the scope of action of the Internal Control over Financial Reporting System implemented.

Control environment: defines the organization and responsibilities of the different stakeholders in relation to the ICFRS.

Methodology of the Internal Control over Financial Reporting System: defines the activities, practices, procedures and technical tools provided for the correct development of the Internal Control over Financial Reporting System implemented. In this sense, the ICFRS Process consists of the following fundamental ones:



Risk identification and assessment



Identification and documentation of key processes and controls



Monitoring and reporting



ICFRS Update

(2) Article 35 of the Regulations of the Board of Directors of the Company.

El SCIIF es un conjunto de procesos que afectan a todos los niveles de la organización y a todo el personal de la Sociedad. Principalmente:

1. CONSEJO DE ADMINISTRACIÓN

Funciones

- ▶ Formular las cuentas anuales y su presentación a la Junta General de accionistas.
- ▶ Determinar la política de control y gestión de riesgos.
- ▶ Dar seguimiento a los sistemas de control interno y de información.
- ▶ Aprobar la información financiera que, por la condición de cotizada, la Sociedad deba hacer pública periódicamente.

Como responsable último de la supervisión del SCIIF, el Consejo de Administración ha establecido la estructura organizativa necesaria que permite su seguimiento mediante el apoyo para dicha tarea en la Comisión de Auditoría y Control.

2. COMISIÓN DE AUDITORÍA Y CONTROL

Funciones

- ▶ Velar por el buen funcionamiento de los sistemas de información y control interno, en particular respecto a los procesos de elaboración e integridad de la información financiera.
- ▶ Conocer y revisar periódicamente el proceso de elaboración y presentación de la información financiera y los sistemas de control y gestión de riesgos internos asociados a los riesgos relevantes de la Sociedad.
- ▶ Presentar recomendaciones o propuestas al Consejo de Administración dirigidas a salvaguardar la integridad de los sistemas de información y control.

En el cumplimiento de estas funciones, la Comisión de Auditoría y Control, debe velar por los siguientes aspectos relativos al SCIIF de la entidad:

- ▶ El cumplimiento de los requisitos normativos.
- ▶ La adecuada delimitación del perímetro de consolidación.
- ▶ La correcta aplicación de los criterios contables.

En el plano de organización de los trabajos del SCIIF, la Comisión de Auditoría y Control es responsable de aprobar qué y cuándo supervisar y cómo evaluar la supervisión SCIIF (aprobación del Plan de trabajo y de supervisión del SCIIF).

3. DIRECCIÓN FINANCIERA

Funciones

- ▶ Diseñar, implementar, evaluar y dar seguimiento global al SCIIF, para lo cual validará el diseño del Plan de trabajo y de supervisión del SCIIF.
- ▶ Reportar sobre el funcionamiento eficaz del SCIIF a la Comisión de Auditoría y Control.
- ▶ Velar por que se ejecuten los debidos programas de formación sobre el SCIIF.

4. RESPONSABLE DEL SCIIF

Funciones

- ▶ Identificar los riesgos de error, omisiones o fraude en la información financiera mediante la matriz de *scoping* (o matriz de alcance) del SCIIF y de documentar el diseño de los controles.
- ▶ Velar por el correcto funcionamiento del SCIIF, para lo cual los responsables de cada proceso/subproceso y controles asociados deben realizar el seguimiento de los mismos reportando dicha información al responsable del SCIIF de Árima.
- ▶ Preparar reportes para la Dirección Financiera, considerando los resultados de los reportes recibidos.
- ▶ Alertar sobre cambios en los escenarios regulatorios y de riesgos de la información financiera.
- ▶ Identificar nuevos riesgos en los procesos.
- ▶ Colaborar en la propuesta de acciones de mejora y resolución de incidencias.

Árima es una compañía comprometida con los más altos estándares de calidad y cumplimiento. Como tal, realiza un seguimiento constante de su Sistema de Control Interno, en línea con su evolución y con las novedades que surgen en el mercado en cuestiones de *reporting*. Con este espíritu, durante 2021 ha profundizado en su Sistema de Control Interno de la Información Financiera (SCIIF), sometiéndolo además a una revisión externa voluntaria para asegurar su eficaz diseño y aportar una mayor transparencia. Esta revisión ha sido llevada a cabo por un equipo de expertos especializados de la firma PwC, obteniendo un resultado satisfactorio y cuyo informe ha sido publicado como parte del Informe Anual de Gobierno Corporativo de 2021.

The ICFRS is a set of processes that affect all levels of the organization and all Company personnel. Mainly:

1. BOARD OF DIRECTORS

Functions

- ▶ To prepare the annual accounts and their presentation to the General Shareholders Meeting
- ▶ To determine the risk control and management policy.
- ▶ To monitor the internal control and information systems.
- ▶ To approve the financial information which, as a listed company, the Company must periodically publish.

As the ultimate responsible for the supervision of the ICFRS, the Board of Directors has established the necessary organizational structure that allows its monitoring through the support of the Audit and Control Committee for this task.

2. AUDIT AND CONTROL COMMITTEE

Functions

- ▶ To ensure the proper functioning of the information and internal control systems, in particular with regard to the preparation and integrity of the financial information.
- ▶ To be aware of and periodically review the process of preparation and presentation of financial information and the internal risk control and management systems associated with the risks associated with the Company's significant risks.
- ▶ Submit recommendations or proposals to the Board of Directors aimed at safeguarding the integrity of the information and control systems.

In the performance of these duties, the Audit and Compliance Committee must ensure the following aspects relating to the company's ICFRS:

- ▶ Compliance with regulatory requirements.
- ▶ Adequate delimitation of the scope of consolidation.
- ▶ The correct application of accounting criteria.

In terms of the organisation of the ICFRS work, the Audit and Compliance Committee is responsible for approving what and when to supervise and how to assess ICFR supervision (approval of the ICFR work and supervision plan).

3. FINANCIAL MANAGEMENT

Functions

- ▶ Design, implement, evaluate, and provide overall monitoring of the ICFR, for which he/she shall validate the design of the SCIIF Work and Monitoring Plan.
- ▶ Report on the effective functioning of the ICFR to the Audit and Control Committee.
- ▶ Ensure that appropriate ICFR training programmes are implemented.

4. ICFRS RESPONSIBLE

Functions

- ▶ Identify the risks of error, omission, or fraud in financial reporting through the ICFRS scoping matrix and documenting the design of controls.
- ▶ Ensure the proper functioning of the ICFRS, for which those responsible for each process/sub-process and associated controls must perform the monitoring thereof, reporting such information to Árima's ICFRS manager.
- ▶ Prepare reports for the Financial Management, considering the results of the reports received.
- ▶ Alert on changes in regulatory and risk scenarios of financial information.
- ▶ Identify new risks in the processes.
- ▶ Collaborate in the proposal of improvement actions and resolution of incidents.

Árima is a company committed to the highest standards of quality and compliance. As such, it constantly monitors its Internal Control System, in line with its evolution and with the new developments that arise in the market in reporting matters. In this spirit, during 2021 it has deepened its Internal Control over Financial Reporting System (ICFRS), also submitting it to a voluntary external review to ensure its effective design and provide greater transparency. This review has been carried out by a team of specialized experts from the firm PwC, obtaining a satisfactory result and whose report has been published as part of the 2021 Annual Corporate Governance Report.