2025

COMPLIANCE COMITTEE REPORT

INDEX

1. DESCRIPTION, RATIONALE AND OBJECTIVES

This Report compiles the main activities carried out by the Compliance Committee of Navantia, S.A., S.M.E. (hereinafter "Navantia", "the Company" or "the Enterprise", interchangeably) in its various areas of action, and includes both the meetings held during financial year 2025 and the matters addressed therein.

Its preparation and submission are in response to the provisions of section 4.1.3 on the "reporting system" of the Compliance Committee Regulations (N-CA-000.5).

This "Compliance Committee Report for financial year 2025" is addressed to Navantia's Board of Directors.

2. OVERALL REVIEW OF FINANCIAL YEAR 2025

During financial year 2025, improvements were made in the deployment of the Compliance culture, and progress was achieved in strengthening the Compliance Management System thanks to the leadership and involvement of the governing bodies and the deployment of risk assessment by Areas, which provides greater visibility in order to establish objectives and actions that lead Navantia towards better risk control.

The most noteworthy aspects implemented during this period were:

- Progress in updating the governance system.
- Conducting the new supplier survey in relation to the objectives set for 2025.
- Updating the Compliance regulatory framework in order to adapt it, among other matters, to current regulations, international standards and the continuous improvement process.
- Renewal of the management system approval certificate under ISO 37001:2016.
- Obtaining the approval certificate for the Criminal Compliance system under UNE 19601:2017.
- Implementation of the 3rd phase of Navantia's Internal Fraud System, through the progressive implementation of the controls planned in the different waves. Likewise, critical fraud processes in the Businesses have been identified and the associated risks analysed, together with the existing or necessary controls for their mitigation.
- Risk assessment by areas and incorporation of new controls for the areas identified as having a higher risk.

These advances would not have been possible without the dedication, effort and professionalism of the Compliance Department and the other company areas that participated.

3. NAVANTIA'S COMPLIANCE SYSTEM

3.1. Regulatory framework

By resolution of Navantia's Board of Directors dated 14 January 2015, the Company's Compliance Management System was approved. It is composed of the following documents, in their latest and most up-to-date versions:

- **Anti-Corruption and Compliance Policy**

This policy reinforces the commitment of the Governing Body and Senior Management to link their ethical values and compliance with current legislation in all countries in which the company operates, with special emphasis on zero tolerance towards corruption and fraud, as well as the commission of other unlawful acts, cooperating with the Justice system.

This policy applies to the Navantia Group, as well as to third parties that interact with it.

The latest review was approved by the Board of Directors in June 2024, in order to adapt it to the UK Bribery Act 2010 and to include the concept of "zero tolerance towards corruption".

- **Navantia Business Code of Conduct** (N-CA-000.01)

This document establishes the standard of conduct that Navantia seeks to observe in all its business activities and applies to the entire Navantia Group.

The Code of Conduct was reviewed and approved by the Board of Directors in May 2025, in connection with the inclusion of the "SOMOS" values and the ethical use of Artificial Intelligence.

- **Compliance Committee Regulations** (N-CA-000.05)

These Regulations define the composition and basic functions of the Compliance Committee, as well as its scope of action and internal operation.

During financial year 2025, review no. 5 of the Regulations was carried out due to the modification of the positions held by the members of the Compliance Committee in accordance with Navantia's organisational changes.

- **Compliance Manual** (N-CA-003)

This Manual details the principles for the management and prevention of offences within Navantia, in accordance with Organic Law 10/1995 of 23 November, on the Criminal Code, and also sets out the proposed structure and functioning of Navantia's control and supervisory bodies.

During financial year 2025, the Compliance Manual was not reviewed.

- **Ethics Channel Policy** (N-CA-005)

This Policy establishes the guiding principles of the Ethics Channel, detailing the channels that may be used to report breaches.

No amendments were made during financial year 2025.

- **Other regulations and procedures**

In addition to the above regulations approved by the Board of Directors, the remaining internal procedures that develop them, and which have been approved by the Compliance Committee, should also be added:

- P-CU-001 Management of conflicts of interest. No amendments were made during financial year 2025.
- P-CU-002 Anti-corruption. No amendments were made during financial year 2025.
- P-CU-003 Crime prevention. No amendments were made during financial year 2025.
- P-CU-004 Special procedure of the Board of Directors for action and decision-making in the event of breaches of the Compliance Management System.

  During financial year 2025, amendments were made in order to include the recommendations submitted by the SEPI Internal Audit.
- P-CU-005 Management of transparency obligations (Law 19/2013). No amendments were made during financial year 2025.
- P-CU-006 Essential reporting on Compliance matters. No amendments were made during financial year 2025.
- Specific Code of Conduct for Business Partners. No amendments were made during financial year 2025.

3.2. Control bodies

In order to achieve the effective operation of the prevention model, it must be periodically verified and, where appropriate, amended when significant breaches of its provisions are identified or when changes occur in the organization, the control structure or the activity carried out by the company.

Navantia has the following bodies that perform control and monitoring functions:

- **Board of Directors:** it is responsible for performing the general supervisory function over the effective operation of the Compliance Committee.

  It also has the power to determine the company's **general policies and strategies**.

- **Compliance Committee:** it is the autonomous initiative and control body entrusted by the Board of Directors with monitoring the operation and observance of the Crime Prevention System, as well as its updating.

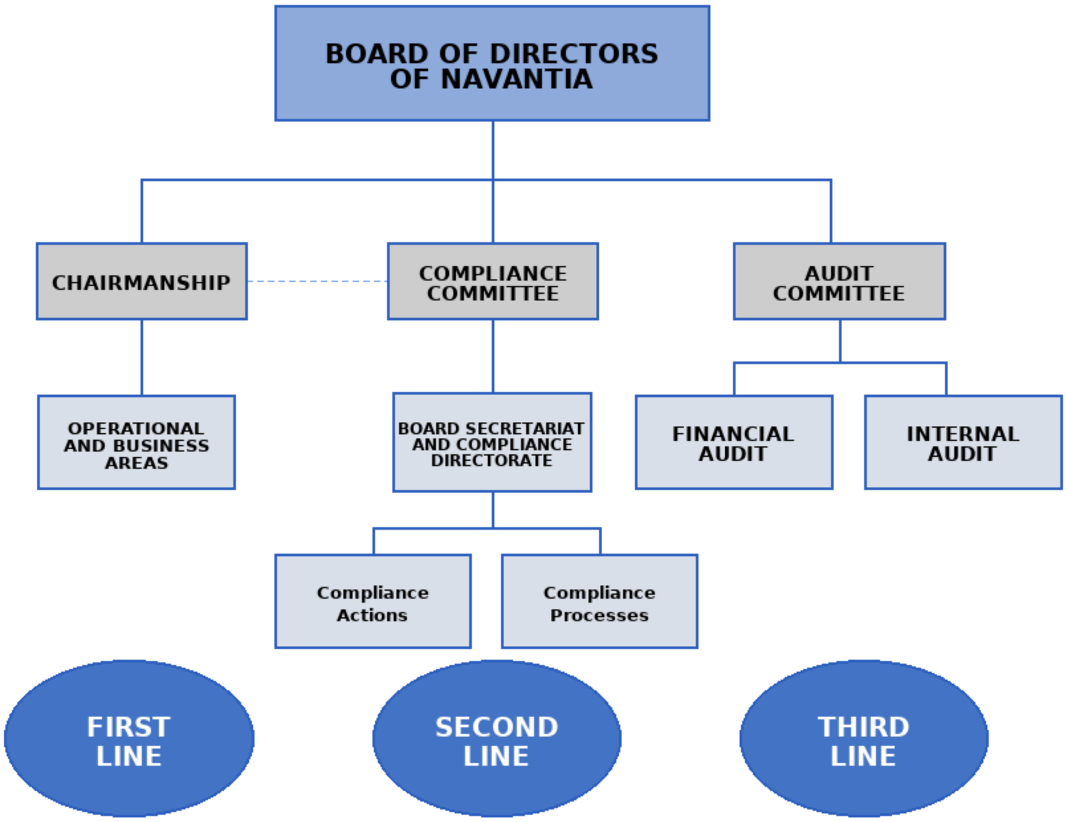
  It must also report on an ordinary and extraordinary basis to the Board of Directors or to the Audit Committee and is responsible for the Internal Reporting System under Law 2/2023.

- **Board Secretariat and Compliance Department:** headed by the chair of the Compliance Committee and to which the Compliance Actions and Compliance Processes managers' report.

- **Compliance Actions Manager:** responsible for the Internal Reporting Channel, actions to detect breaches, their investigation and control, as well as monitoring the organizational and personnel-related measures adopted in response to breaches or deficiencies detected.

- **Compliance Processes Manager:** responsible for prevention, assessment and management of criminal risks and other compliance risks, management of the IT system for internal controls, due diligence activities, promotion, dissemination and support for Compliance training, and supervision and monitoring of the Compliance System of subsidiaries.

The hierarchical and functional structure of these bodies, organized by lines of defense, is shown below:



The "Three Lines" model establishes that the controls implemented by the operational departments constitute the first line of defense in risk management, including corruption risks. The Compliance Committee constitutes the second line, while the Internal Audit Department is the third line.

- **First line (the Business):** this line maintains the primary contact with customers, suppliers and partners. They live with the risk and must therefore be sufficiently trained to understand not only what they need to request, but also why, so that, once the necessary information is available, the customer can be identified, their source of income understood, and their risk properly assessed.
- **Second line (Compliance Committee):** its responsibility includes implementing policies, procedures and controls that mitigate the risk of breaches of legal requirements or self-imposed rules by the Company. These tasks must be reinforced through ongoing training, a robust structure and tools that help automate the control and monitoring of relationships.
- **Third line (Internal Audit):** this line is responsible for auditing the work performed by the first two lines.

As a guarantee of independence within the organisation, the Internal Audit and Compliance functions report hierarchically to Navantia's chairmanship and report to the Board of Directors.

4. COMPLIANCE COMMITTEE

The Compliance Committee was established on 20 July 2018, following the amendment of the Criminal Compliance System by the Board of Directors, assuming the functions of an **autonomous initiative and control body**, which until then had been performed by the Audit Committee and the Compliance Unit.

The purpose of the Compliance Committee is to ensure the ethical and legal conduct of Navantia's professionals.

Its work is mainly aimed at promoting and coordinating the implementation, supervision and control of the Compliance Management System. Accordingly, the Compliance Committee will seek to prevent inappropriate behaviour and, where applicable, detect it and respond diligently.

The Compliance Committee, as a control body, has a direct reporting line to Navantia's Board of Directors.

However, the Compliance Committee may periodically inform the Audit Committee of the activities carried out as a whole and may even request its assessment of matters of greater significance or risk.

4.1. Functions and responsibilities

The Compliance Committee has entrusted the operational performance of its functions to the Compliance Department.

The main responsibilities of the Compliance Committee, as set out in the Compliance Committee Regulations (N-CA-000.05), are as follows:

- **Supervision and control of compliance with the Business Code of Conduct**

  With regard to compliance with and updating the Business Code of Conduct, the following tasks correspond to the Committee:

  - Ensure that the system of values adopted in the Business Code of Conduct is up to date and propose any updates and integration that may be necessary.
  - Comply with and enforce the Business Code of Conduct.
  - Ensure the effective communication and dissemination of the Code of Conduct, being responsible for the adoption and effective implementation of the Communication Plan.
  - Analyse and propose to the Internal Audit Department the assessment actions that could be periodically incorporated into the annual Audit Plans to verify Navantia professionals' knowledge of the Business Code of Conduct, as well as their degree of compliance with it.

- Receive and process all types of written communications containing questions or requests for clarification regarding the application of the Business Code of Conduct.

- Receive and process any questions regarding conflicts of interest that may arise among Navantia professionals.

- Resolve any doubts that may arise regarding the application and interpretation of the Business Code of Conduct.

- Manage and process the resolution of reports of breaches of the Business Code of Conduct received through the Ethics Channel. In carrying out these actions, and where the subject matter of the report makes it appropriate, the Committee may request the collaboration of other company bodies, which shall carry out verification actions within the scope of their powers and in accordance with the principles of confidentiality, objectivity and independence. The bodies appointed by the Compliance Committee to analyse reports may in turn contact any other Navantia body, which shall always be required to provide the information necessary to investigate the report, provided there is no legal prohibition preventing this.

- Decide on the measures to be adopted following the investigations carried out and approve any disciplinary sanctions that may be proposed by the Human Resources Department in accordance with the disciplinary procedure.

- Propose, where appropriate, the relevant disciplinary measures in response to potential breaches, always referring them to the Human Resources Department for their execution, in accordance with the disciplinary procedure and applicable labour regulations.

- In any event, the Human Resources Department shall act in coordination with the Compliance Committee to ensure that the disciplinary measures ultimately imposed are consistent with the Compliance Management System.

- **Supervision and control of compliance with the Compliance Management System.**

  Specifically, the responsibilities of the Compliance Committee in this area are as follows:

  - Ensure the dissemination of the principles of the Compliance System within the Company. Promote and supervise initiatives aimed at spreading knowledge and understanding of the control system.

  - Supervise the operation of the Compliance Management System.

  - Analyse and approve action plans and periodic review/control/audit plans for the model. Request additional reviews if deemed necessary.

  - Report periodically, at least once a year, and whenever it deems appropriate, to Navantia's Board of Directors on the activities carried out.

  - Supervise the updating of the register of gifts given/received by Navantia or its personnel.

  - Coordinate the compliance functions in each of Navantia's subsidiaries and investee companies, and receive the periodic reports, whether quarterly or half-yearly, arising from their activity.

  - Manage Navantia's Ethics Channel and coordinate the investigation and resolution of reported facts for the purpose of:

    - ✓ Agree to close the report, recording the reason for doing so.

    - ✓ If indications of potentially criminal conduct are confirmed, refer the matter to the competent authority.

    - ✓ Bring the most relevant facts to the attention of the Board of Directors.

    - ✓ Adopt the appropriate improvement measures regarding the Company's compliance management system.

    - ✓ Propose, where appropriate, the relevant disciplinary measures in response to potential breaches, always referring them to the Human Resources Department for their execution, in accordance with the disciplinary procedure and applicable labour regulations.

Compliance risks related to occupational risk prevention and the environment are not managed by the Compliance Committee, as these matters are regulated by sector-specific legislation, which requires the full integration of prevention of these risks into management processes and the creation of worker supervision, control and participation bodies that define the policy on prevention and the environment and supervise how it is implemented.

Therefore, in order to avoid duplication of functions in the areas of occupational risk prevention and the environment, the Compliance Committee shall only act as supervisor of those controls that, where applicable, could have an impact on the Compliance Management System, while supervision and control of the compliance model in relation to occupational risk prevention and the environment shall fall to the bodies appointed for that purpose.

The Compliance Committee shall be responsible for filing and safeguarding all documentation it receives in the exercise of its functions, including minutes, reports and assessments, for a minimum period of ten years.

4.2. Composition

In accordance with the Compliance Committee Regulations, the Compliance Committee is established as a collegiate body composed of:

- The holder of the Board Secretariat and Compliance Department position (Chair of the Compliance Committee).
- The holder of the Finance Department position.
- The holder of the Legal Affairs Department position.
- The holder of the Human Resources Department position.
- The holder of the Technology and Digital Transformation Department position.

The Compliance Committee is structured into a chair and ordinary members. Its members must have the knowledge, skills and experience appropriate to the functions they are called upon to perform and shall be appointed by Navantia's Board of Directors.

The Compliance Committee also has a non-member secretary, who is a Navantia employee assigned to the Board Secretariat and Compliance Department.

4.3. Meetings and calls

The Compliance Committee Regulations establish that the Committee shall meet ordinarily on a quarterly basis. Meetings shall be scheduled prior to being held in a calendar established for that purpose.

Likewise, the Compliance Committee shall meet on an extraordinary basis whenever circumstances so require, with such extraordinary meetings being called as soon as possible.

Compliance Committee meetings shall be validly constituted when more than half of its members attend, either in person or by proxy, unless it is not possible to reach that number due to conflicts of interest. Meetings shall be chaired by the chair of the Compliance Committee. In their absence, they shall be chaired by the member with the longest service in the Company.

The chair of the Compliance Committee may require the attendance of any other member of the organisation or even of companies' majority-owned by Navantia.

4.4. Adoption of resolutions

The resolutions of the Compliance Committee are adopted by the favourable vote of the majority of the members present or represented. Resolutions shall be recorded in signed minutes, which shall be prepared and kept by the secretary in a minute book.

The statements issued by the Compliance Committee, whether as opinions or recommendations, shall in all cases be disseminated internally as determined by the Compliance Committee on each occasion.

4.5. Reporting system

The Compliance Committee shall report ordinarily, on an annual basis, to Navantia's Board of Directors, to which it shall submit a report on its main activities, after informing the Corporate Management Committee.

Likewise, the Compliance Committee may report extraordinarily at any time when it considers that there is a relevant matter that should be brought to the attention of the Board of Directors or, where appropriate, the Audit Committee of the Board of Directors.

5. COMPLIANCE COMMITTEE ACTIVITY 2025

As of 31 December 2025, the Compliance Committee was composed of the following members:

Chair	Appointment
Miguel Orozco Giménez	16 February 2021

Members	Appointment
Patricia de Paredes Alonso	21 November 2022
Alejandro Rubio González	16 February 2021
Diego de Santiago Lareo	24 May 2024
Ana Micaela Moya Gutiérrez	7 July 2025

Non-member secretary[1]	Appointment
Paul Rodríguez Pena	30 June 2015

During financial year 2025, the Compliance Committee held 11 ordinary meetings, 3 extraordinary meetings and adopted 2 resolutions without a meeting.

6. COMPLIANCE WITH 2025 OBJECTIVES

The level of achievement of the Compliance Department's objectives for financial year 2025, approved by the Compliance Committee, was as follows:

[1] When the Compliance Committee acts in its capacity as the body responsible for Navantia's Internal Reporting System, it shall act as an additional member of the Compliance Committee, with full speaking and voting rights.

<table>
<tr><th>DEPARTMENT OBJECTIVES</th><th>TARGET DATE</th><th>ACHIEVED DATE</th><th>% ACHIEVEMENT</th></tr>
<tr><td>Carry out the implementation of the 3rd phase of Navantia's Internal Fraud System (definition of the fraud risk map based on business processes, definition and implementation of anti-fraud controls) and submit to the Compliance Committee a report on the actions carried out and the level of execution.</td><td>31/12/2025</td><td>30/11/2025</td><td>100 %</td></tr>
<tr><td colspan="4">The actions carried out during 2025 to achieve this objective were as follows:

• Implement the controls defined in the second phase (first wave).
• Implement the second wave of controls.
• Define critical fraud processes in the Businesses.
• Identify fraud risks and controls arising from the critical processes of the Businesses.
• Submit the proposed action plan to the Compliance Committee.

The approach consists of understanding and analysing all company processes in order to identify those that are critical from a fraud perspective, detect associated risks and define the corresponding fraud controls. Based on this analysis, the scope, prioritisation, methodology, phasing and implementation deadlines are established, identifying and confirming the controls to be deployed. The process is completed by monitoring the build and testing in the Development environment, transferring the controls to Production with the corresponding parameterisation and configuration, and finally executing and validating the controls in the Production environment to ensure their proper operation.</td></tr>
<tr><td>Implement a Global Compliance Management System in line with the requirements of ISO 37301 or UNE 19601 certifications, submit its correct design and implementation to an external audit, and present the audit results to the Compliance Committee as a prior step before starting the certification process under the relevant standard(s).</td><td>31/12/2025</td><td>31/07/2025</td><td>100 %</td></tr>
<tr><td colspan="4">The actions carried out during 2025 to achieve this objective were as follows:

• Review of the Compliance Management System in line with the certifications.
• Carry out and submit to the Compliance Committee an individualised Compliance risk assessment for each of the areas with a risk level above low.
• Submit its correct design and implementation to an external audit.
• Present the audit results to the Compliance Committee.

The work includes analysing the gap analysis and the action plan approved by the Compliance Committee, executing the resulting actions and requesting external consultants to review the Compliance Management System. In parallel, areas with a risk level above low are analysed, the risk assessment is carried out, recorded in the TeamMate+ tool and submitted to the Compliance Committee. The process is completed with the management of the external audit by the Quality area, including the engagement and scheduling of the audit team, the provision of preliminary documentation, execution and closure of the audit, and formal receipt of the results issued by the auditors.</td></tr>
<tr><td>Deploy the Compliance Supervision and Reporting System of the Navantia Group and submit to the Compliance Committee a report on the actions carried out and the level of execution.</td><td>31/12/2025</td><td>30/11/2025</td><td>100 %</td></tr>
<tr><td colspan="4">In order to achieve the objective, the following tasks were carried out:

• Define the individualised action plan for each subsidiary (majority-owned investees).
• Submit the Action Plan to the Compliance Committee for approval.
• Communicate and execute the Action Plan for each subsidiary (majority-owned investees).
• Prepare a report on the actions carried out and their level of execution.
• Submit the proposed action report to the Compliance Committee.

The work consists of analysing the Compliance regulations applicable to Navantia UK, the majority-owned international subsidiaries (Navantia Arabia and Navantia Australia) and the majority-owned national subsidiaries, defining a specific</td></tr>
</table>

<table>
<tr><td colspan="4">Action Plan in each case, as well as a reduced reporting and supervision plan for minority investees, executed from Navantia. These Action Plans are communicated to the national and international subsidiaries and supported through meetings to facilitate their correct understanding and application, subsequently proceeding with their execution. As the final step in the process, a consolidated report is prepared setting out all the actions carried out.</td></tr>
<tr><td>Define and submit to the Compliance Committee a new supervision system for higher-risk business partners in Compliance matters.</td><td>31/12/2025</td><td>30/11/2025</td><td>100 %</td></tr>
<tr><td colspan="4">The actions carried out during 2025 to achieve this objective were as follows:

• Prepare an analysis report on business partners and analyse which of them have a Compliance Management System and whether they have had any Compliance-related incidents in the last five years (alert system).
• Define and carry out a performance assessment on ethical culture and Compliance (survey) for business partners.
• Prepare a conclusions report and define the Business Partner Review System.
• Submit the proposed review of business partner supervision to the Compliance Committee.

The process covers the analysis of Navantia’s business partners in order to identify which ones should be assessed, determine whether they have a Compliance Management System and detect any potential incidents in this area. To this end, a survey is designed and deployed using Microsoft Dynamics 365, including the definition of questions, their upload into the tool, functionality testing, obtaining contacts, sending the survey to the target companies, granting deadlines and sending reminders. Finally, the results obtained are analysed jointly, conclusions are drawn and a review and monitoring system for business partners is defined based on the risks and evidence identified.</td></tr>
<tr><td>Implement actions arising from the ISO 37001 and SEPI audits (Ethics Channel) in order to ensure compliance.</td><td>31/12/2025</td><td>30/06/2025</td><td>100%</td></tr>
<tr><td colspan="4">The actions carried out during 2025 to achieve this objective were as follows:

• (ISO 37001 Internal Audit) Include in the table of contents of reports to Senior Management the section structure required under the reference standard, as this could facilitate and ensure compliance.
• (ISO 37001 Internal Audit) According to personnel functions and risks, determine how often staff training must be renewed.
• (ISO 37001 External Audit) It is recommended to specify a channel or means to be used when the reported person is the personnel responsible for handling reports.
• (SEPI Audit. Ethics Channel) Comply with the recommendations arising from this audit, which have been registered by Navantia’s Internal Audit Department in TeamMate+.

The 2024 Report was already prepared in accordance with the structure established by ISO 37001, thereby consolidating its alignment with Compliance standards. Likewise, with regard to training, the frequency with which staff training must be renewed is included in the 2025 Training Plan and its inclusion in internal regulations is planned, the latter being postponed to 2026 to take advantage of future amendments. In addition, the management channel for the Ethics Channel in the event of conflicts of interest is agreed in coordination with Internal Audit and the relevant regulations are amended.

The recommendations of the SEPI Internal Audit have already been implemented, with only one matter remaining pending —and postponed to 2026— namely the implementation of a secure, long-term system for the preservation of closed internal investigation files, replacing the use of encrypted USB drives and ensuring the confidentiality and recoverability of the information.</td></tr>
</table>

7. DISCLOSURE/TRAINING ON CRIME PREVENTION AND INTEGRITY

Compliance must be promoted from the highest levels of the organisation, strengthening the environment and spirit of regulatory compliance. In this regard, and as a complement to senior management commitment, a decisive aspect of compliance models is the training and awareness-raising of employees and related parties.

Thus, the U.S. Federal Sentencing Guidelines, section 8B2.1 (4 A/B), establish that: "The organisation shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of its ethics and compliance programme, to the members of the governing authority, high-level personnel, personnel with substantial authority in this area, employees and, where appropriate, agents and representatives. This shall be carried out through effective training programmes and by otherwise disseminating information appropriate to such individuals' respective roles and responsibilities."

Furthermore, ISO 37001/37301 standards state that if the people working in the organisation are not aware of the Compliance policy, its importance within the Compliance Management System and the implications of failing to meet the requirements, the system will never function properly.

7.1. Communication and Disclosure Plan on Compliance matters

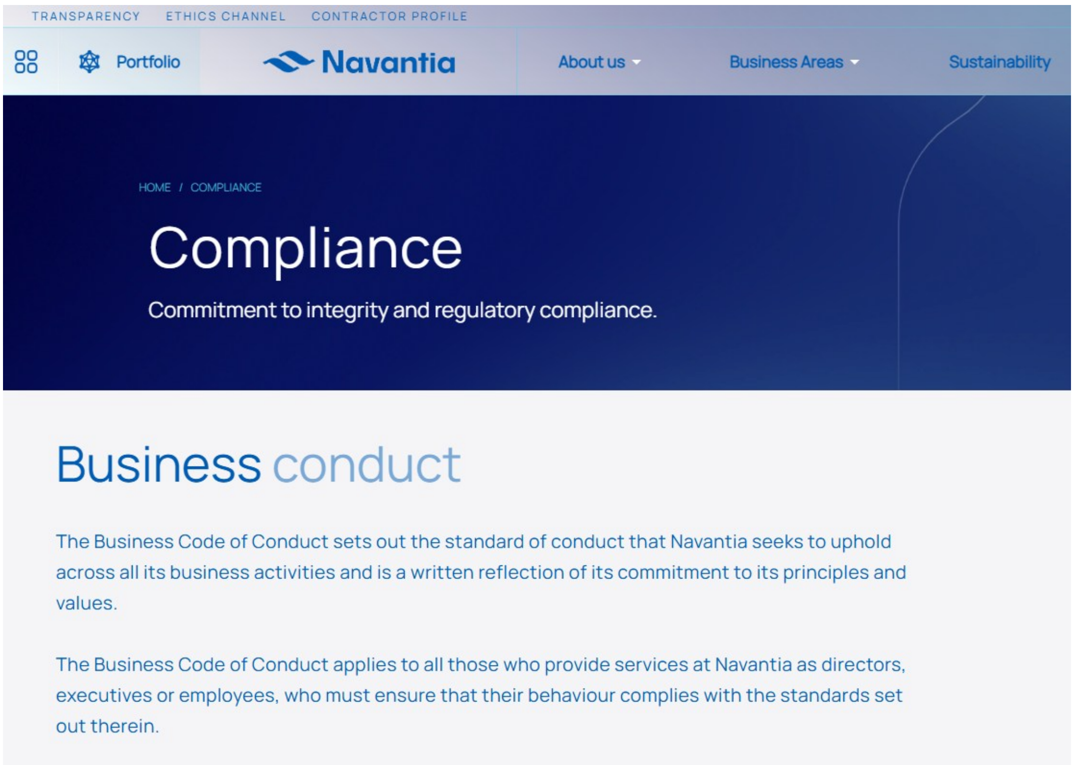
Communication and disclosure, within a compliance risk management system based on ISO standards, is a highly important requirement, but also a necessity. A **Compliance Communication and Disclosure Plan** that ensures the message reaches employees, customers, suppliers and all stakeholders therefore becomes an integral and essential element of the management system.

7.1.1. Communication and disclosure during 2025

Efficient communication and dissemination of Compliance matters to the organisation's personnel, as well as to third parties, is one of the main objectives of the Compliance Department. The Communication and Disclosure Plan has focused on disseminating and raising awareness of all Navantia's policies and objectives in relation to compliance and anti-corruption, as this is considered essential for stakeholders to act in accordance with them. The target audiences are all employees, including lower levels of the organisation and those with limited access to electronic devices, as well as trade unions, shareholders (SEPI and subsidiaries) and business partners. In addition, the Compliance Department has carried out other external dissemination activities to raise awareness of Navantia's Compliance function externally (e.g. compliance associations, participation in webinars, improving visibility on the corporate website, printing posters, etc.).

- **EXTERNAL:**

- **Corporate website**: Compliance is integrated into the Good Governance menu.



During financial year 2025, continuous updates were made to the website, both to procedures and content, to improve transparency, including the inclusion of an annual stakeholder report with information on Compliance activity.

- **Compliance associations:** Navantia actively participates in Compliance associations in order to disseminate the Compliance culture and convey its importance for Navantia to the various stakeholders.

  Navantia belongs to:

  ✓ The Public Sector working group, together with other state-owned companies, where various current Compliance-related topics are addressed.

  ✓ Spanish Compliance Association (ASCOM): Navantia has been a member of this association since 2022.

- **Webinars/talks/courses organised by external companies/associations**

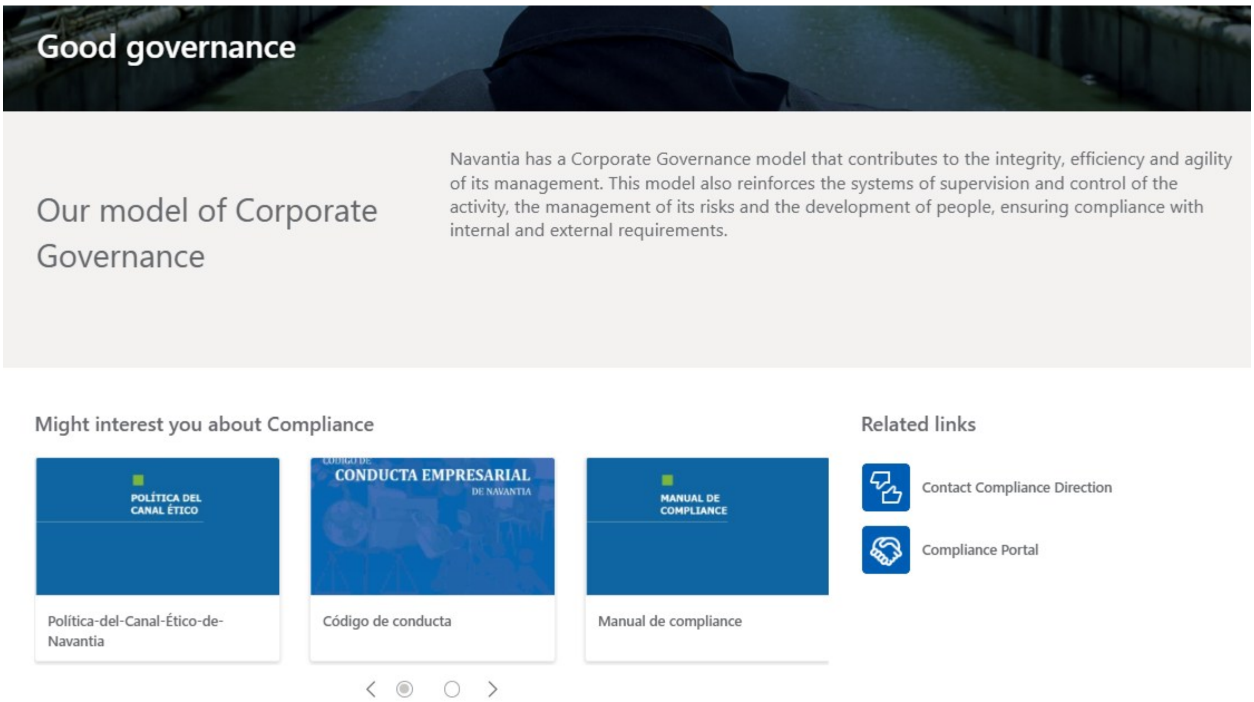
  Navantia will actively participate in any events offered to it, in order to promote Navantia's activity in relation to Compliance.

  Among these, particular mention should be made of the participation of Navantia's Compliance Officer, Paul Rodríguez Pena, as a speaker at the Compliance Congress, organised by the Lugo Provincial Council under the title "Regulatory compliance under debate", and at the "2nd Corporate Integrity Conference: Public Integrity and Compliance", organised by the Ethical Conduct Observatory of the Directorate-General of the Guardia Civil.

- **INTERNAL:**

- **Good Governance section on the intranet / Compliance banner:**

  The company intranet includes the "Good Governance" section, where all Compliance and Privacy content is available.

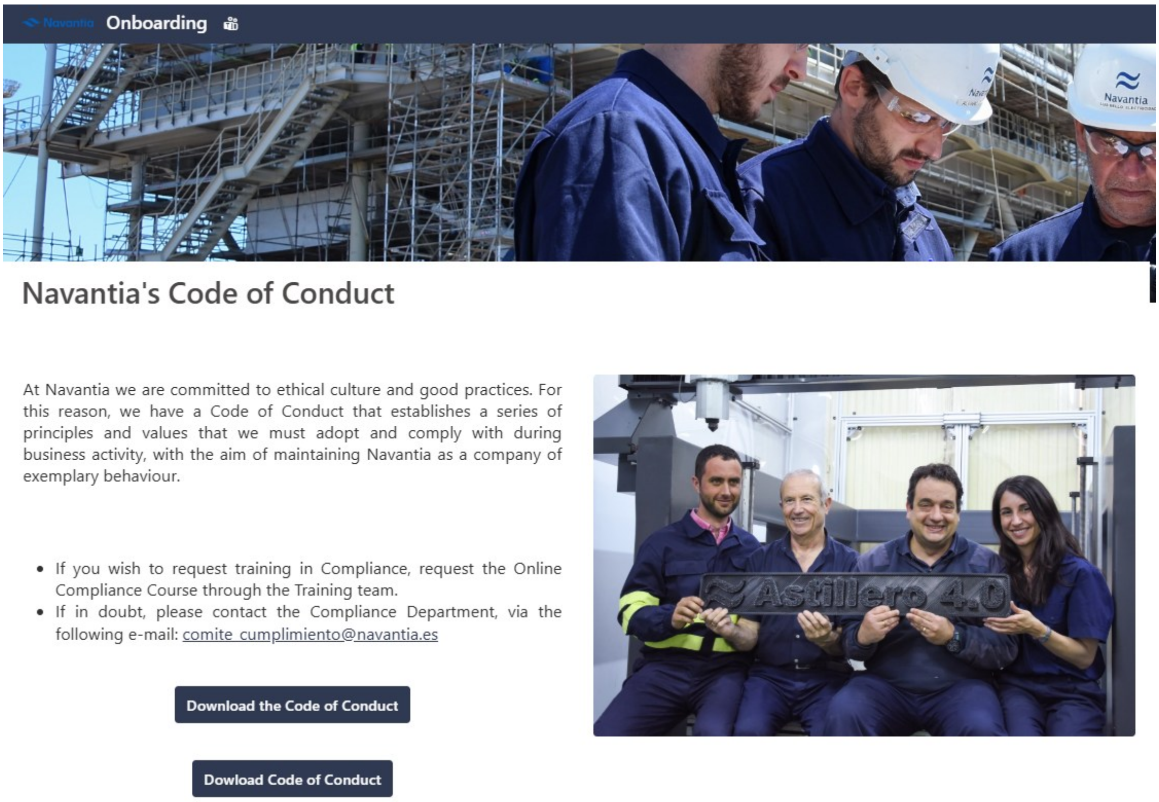


- **Cuadern@/ Periscopio:** during financial year 2025, news items and interviews related to the Compliance Management System were periodically published in **Periscopio/Cuadern@.**

By way of example, a news item is attached with information related to Compliance risks ("What is a compliance risk? Learn about them to avoid legal sanctions and financial losses"), which received almost 500 views.

- **Compliance support and assistance to Navantia's shareholder/subsidiaries/investees**
- **"Onboarding" portal:**

As a result of the existence of the "Onboarding" portal in Periscopio, Navantia has a Compliance section within it.



- **Maintenance of Compliance posters**

During financial year 2025, Navantia maintained Compliance dissemination posters, making it possible to physically consult the Anti-Corruption and Compliance Policy and the Business Code of Conduct. In addition, a QR code is included that provides direct access to the Compliance section on the company's website, so that additional information may be consulted. However, at the end of financial year 2025, the Compliance Department began a process to update the design of the posters in both physical and digital formats.

7.1.2. Communication and disclosure on Compliance matters 2026

Once again, Navantia undertakes to provide effective communication that improves engagement and helps achieve the proposed Compliance objectives. To this end, the Compliance Committee approved a Communication and Disclosure Plan on Compliance matters for financial year 2026, extendable to 2027.

The Communication Plan is aimed at different stakeholders, including employees, trade unions, the shareholder, business partners, public administrations, the media, customers, etc.:

DATE	ACTION	LOCATION	RECIPIENTS
Quarterly	Articles on various Compliance topics: • Ethics Channel • Gifts Policy • Conflicts of Interest • Risky Relationships • Due Diligence	Periscopio and Cuadern@	Navantia Employees
Annual	Communication and acknowledgment of awareness and compliance with the Code of Business Conduct	SAP GRC/Printed format	Navantia Employees
Annual	Performance Evaluation Survey	Microsoft Dynamics 365	Business Partners
Ongoing / Quarterly Review	Maintenance and update of signage and awareness materials (physical and digital): • Ethics Hotline • Gifts Policy • Conflicts of Interest • Risky Relationships • Due Diligence	Physical (Cartagena Shipyard, Cádiz Bay, Ferrol Estuary, Headquarters) and Digital (Navantia Channel)	Navantia Employees, Workers' Councils and Business Partners
Quarterly	Compliance Awareness Session	Cartagena Shipyard, Cádiz Bay, Ferrol Estuary, Headquarters	Navantia Employees, Workers' Councils and Business Partners
Ongoing / Quarterly Update	Maintenance and update of information published on the website (Compliance / Ethics Hotline / Transparency)	Web	Everyone
Upon Request	Navantia's participation in Compliance-related talks, conferences and working groups	Various	Everyone
Ongoing / Quarterly Update	Compliance awareness for new hires	Onboarding Portal / New Hire Welcome Sessions	New Navantia Employees
Upon Request	Support and advice on matters related to the Compliance Management System	Various	Shareholder (SEPI) and Subsidiaries
Annual	Distribution and reminder communications regarding compliance with the Code of Conduct in dealings with Navantia, with particular emphasis on the Gifts Policy and the Ethics Hotline	Various	Business Partners

For any communication action that arises subsequently and is not included in this Plan, a specific Communication Plan will be prepared.

7.2. Compliance training

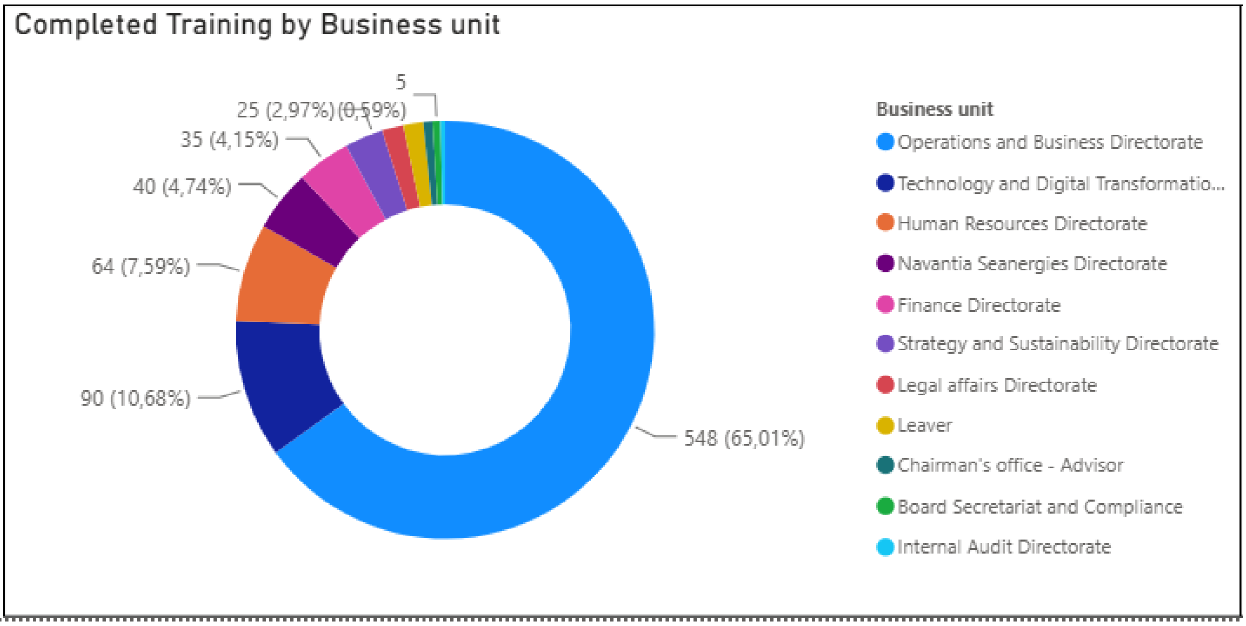
Training, like communication, is highly important within the Compliance function. Navantia therefore undertakes to provide quality training that ensures regulatory compliance and business ethics.

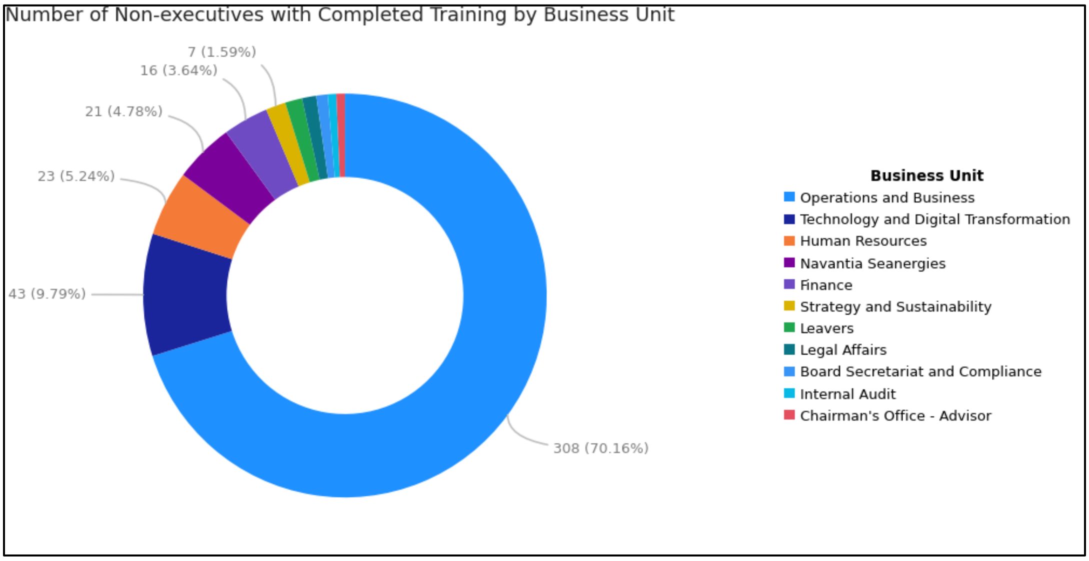
7.2.1. Compliance training for employees during 2025

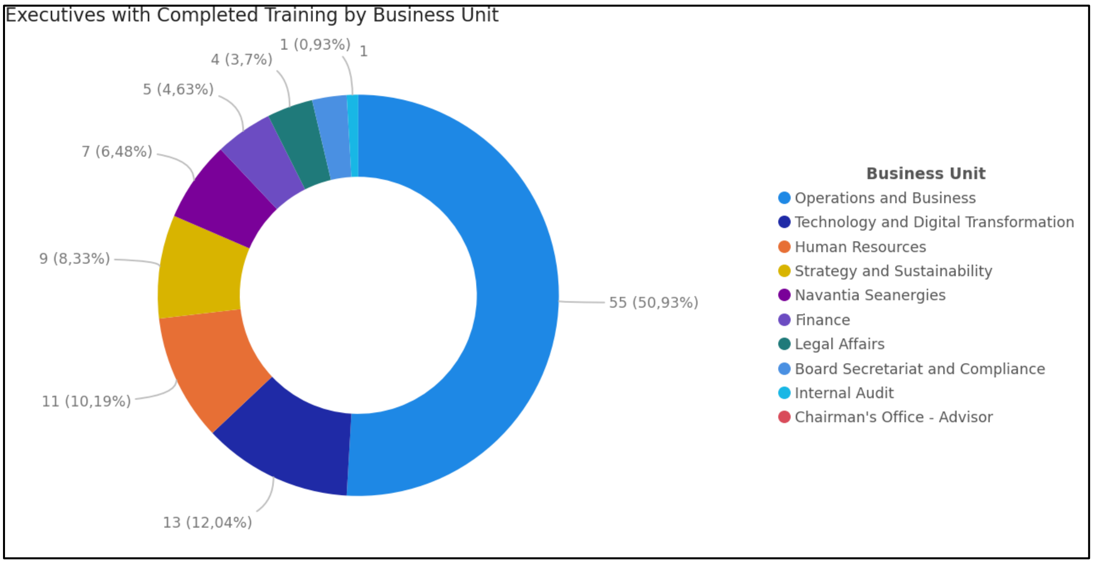
Compliance training for the organisation's personnel has been prepared and delivered by personnel from the Compliance area. The content of each of these actions has been developed on a tailored and individualised basis in order to adapt it to the employees to whom it was addressed and to the specific risks of each department/business.

During financial year 2025, several training actions were carried out, with particular emphasis on personnel with a risk level above low, who were invited to an online Compliance and Anti-Corruption course. In addition to the online Compliance and Anti-Corruption course aimed at all personnel with a risk level above low for 2025, Navantia provided specific training in those areas/functions according to risk, such as the Business Compliance Course for the Purchasing department, anti-corruption training for the Commercial area and specific training for Senior Management personnel and Board members. An internal role-playing training course on compliance was also proposed and delivered to Navantia employees.

The above-mentioned training actions produced the following data:







7.2.2. Training for members of the Compliance Department

One of the requirements of the Compliance Management System is the training of the members of the Compliance Department. Accordingly, in 2025, employees of that Department completed several training courses, notably the Specialisation Programme in Compliance, completed by the Risk Monitoring and Control Senior Specialist, who obtained the CESCOM certification.

On the other hand, taking into account the relevance of Artificial Intelligence (AI), special AI training should be highlighted, completed by all members of the Compliance Department, concerning the new European regulations, more specifically Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation).

Likewise, the members of the Compliance Department have completed individualised training in various areas:

- Power BI course as a way to develop dashboards related to compliance.
- Specialised course on Corruption and Anti-Fraud.
- Training on the presentation and dissemination of Compliance.

- Classified information course.
- Influence impact course: how to be more persuasive.
- CESCOM certificate maintenance course.

7.2.3. Compliance Training Plan for 2026

Training plans must include different types of content and approaches depending on the target audience. To facilitate understanding of the documents that make up Compliance in relation to fraud and corruption, it is advisable to prepare teaching materials that clearly explain the principles and rules guiding the company's activity, as well as examples applied specifically to the company.

Training actions must take into account the audience to which they are addressed:

- **Management personnel** or positions with personnel under their responsibility must complete courses whose message encourages **the exponential expansion of the compliance culture**.
- **Personnel** whose competence or role has a **closer relationship** with **risk** management or with the assumption of responsibility, such as representatives, must receive **more incisive training** on those aspects considered key to the proper functioning of the model.
- **All other personnel** who, in their day-to-day duties, must keep in mind compliance with the law and the principles and values of the **Code of Conduct** that Navantia seeks to observe.

Following the above, the Compliance Committee has defined, in collaboration with the Human Resources Department, the following Training Plan for 2025:

Course	Planned date	Provider	Duration (hours)	Format	Expected employees
Compliance and Anti-Corruption (Generic)	Throughout the year	External	2	Online platform	All personnel
Compliance (Procurement and Contract Managers)	Flexible / To be determined	Internal	2	In-person	300
Anti-Corruption (Commercial Department)	Fourth Quarter	Internal / External	2	In-person / Webinar	30
Role-Playing Workshop	Third Quarter	Internal	2	In-person / Webinar	50
Specific Training for Personnel Exposed to Certain Risks (including corruption and other UNE-ISO 19601 compliance risks)	Flexible / To be determined	External	2	Online/Webinar	100
Specific Training for Senior Management and Board Members	Fourth Quarter	External	2	Webinar	20

It should also be noted that the Training Plan establishes which personnel must renew Compliance training and how often.

8. DUE DILIGENCE PROCESSES

The Spanish Criminal Code establishes that companies may be exempt from potential criminal liability where a criminal risk prevention programme has been effectively implemented within the organisation and there has been no omission in the supervision, monitoring and control functions.

The legislator's intention is to transfer to the company responsibility for not having implemented internal control mechanisms over employees and executives that allow for clear and effective communication of the "rules of the game", the rules of conduct in representation and action on behalf of the company in the case of executives, and also with regard to employees acting under their authority.

Accordingly, the absence of "proper control" or "due diligence" in the legally assigned function of preventing the commission of offences by the company's executives and employees is penalised.

8.1. Due diligence on employees or executives

According to letter h) of article 249 bis of the current consolidated text of the Spanish Companies Act, the appointment of senior management personnel reporting directly to Navantia's executive chairmanship falls to the Board of Directors, which is also entrusted with setting their remuneration.

Without prejudice to the foregoing, before: a) hiring or promoting personnel excluded from the scope of the Collective Bargaining Agreement, b) granting powers of representation by the Board of Directors, c) appointing directors of investee companies/subsidiaries or, where applicable, d) appointing manager(s) of temporary joint ventures, the Compliance Committee verifies that the person has not been convicted by final judgment in any proceedings or investigation concerning corruption, and that they are committed to and willing to comply with Navantia's Business Code of Conduct.

This verification is carried out through[2]:

- Completion of the integrity questionnaire.
- Criminal Record Certificate.
- Screening of the candidate in Compliance and corporate matters.

During financial year 2025, the Compliance Department carried out 38 due diligence procedures on different executives/employees.

8.2. Due diligence on third parties

Navantia must conduct a legal review of third parties with whom it intends to maintain or already maintains a business relationship, regardless of whether they are representatives, agents, consultants, suppliers, other intermediaries, partners, contractors or main subcontractors, distributors, etc., in order to assess the corruption risk before entering into business and throughout the duration of such business.

In general terms, exercising due diligence or proper control over those who interact with Navantia is a very important part of the preventive measures that a company may adopt to prevent reputational, operational and legal risks.

Carrying out this due diligence or proper control is therefore entirely necessary, since otherwise, in the case of offences that could be committed by third parties in the performance of activities carried out on behalf of and for the benefit of Navantia, Navantia could be declared criminally liable for the commission of such offences under article 31 bis of the Spanish Criminal Code, with the resulting economic and reputational cost for the company. Proper due diligence by Navantia helps avoid or minimise these risks.

[2] Such documents shall be made available to the Compliance Department prior to any hiring, promotion, granting of powers of attorney or, where applicable, the corresponding appointment.

The legal review is carried out in accordance with the principles set out in the Anti-Corruption Regulations and in any other policy specifically designed for particular business/risk areas. These reviews may be carried out by Navantia personnel or by engaging specialised companies or professionals.

- **LOW RISK.** Low risk is understood to exist when engaging a third party for business in which the end customer is a public-law entity of the European Union or of third countries with a CPI score equal to or above 80 points, and for business whose end customer is a private-law entity with registered office within the European Union or in third countries with a CPI score equal to or above 60 points.

- **MEDIUM RISK.** Medium risk is understood to exist when engaging third parties for business in which the end customer is a public-law entity of countries with a CPI score equal to or above 50 points, and for business in which the end customer is a private-law entity domiciled in countries with a CPI score equal to or above 40 points.

- **HIGH RISK.** High risk is understood to exist when engaging third parties for business in which the end customer is a public-law entity of countries with a CPI score below 50 points, and for business in which the end customer is a private-law entity domiciled in countries with a CPI score below 40 points or in countries considered tax havens.

For the proper assessment of the aforementioned country risk in relation to corruption and money laundering, in addition to the "Corruption Perceptions Index (CPI)" prepared by Transparency International, the "list of tax havens included in Royal Decree 1080/1991 of 5 July", as well as the current "annual Fragile States Index" of The Fund for Peace, and whether sanctions have been imposed by international organisations, shall also be consulted.

Other factors to be taken into account when determining the third party's risk level are:

- Experience in the industry and its history/reputation regarding corruption.
- The size and scale of the third party and the third party's reputation for integrity.
- Previous history/experience of a business relationship with Navantia.
- Whether the third party is not well known to Navantia.
- The size of the business transaction.
- Whether the third party will deal with public officials on behalf of Navantia.
- Whether the owner, shareholder, director, executive or partner of the third party has been or may be considered a public official.
- Whether the third party is an established entity with significant customers or a newly created company.

During financial year 2025, the Compliance Department carried out 178 due diligence procedures:

- 28 due diligence procedures on agents/intermediaries/lobbies prior to signing a contract or renewing an existing one. There were no Compliance-related incidents to highlight.

- 18 due diligence procedures on agents/intermediaries/lobbies prior to payment of a success fee for a firm contract. There were no Compliance-related incidents to highlight.

- 80 due diligence procedures prior to signing a commercial agreement with 80 business partners.

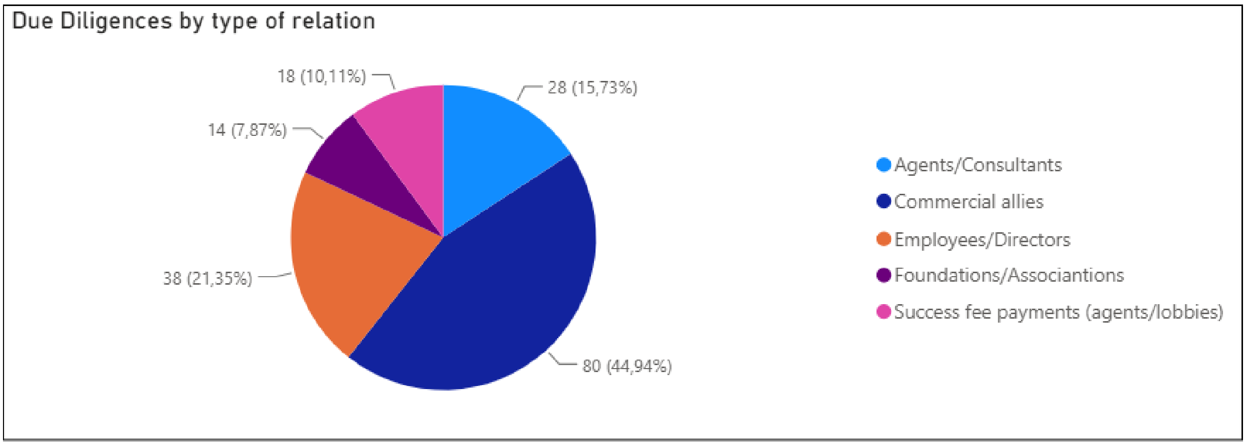
  Of the 80 due diligence procedures on business partners, incidents were reported in only one case.

- 14 due diligence procedures prior to joining an association or non-profit organisation, or prior to making payments to such entities under a collaboration or sponsorship agreement. There were no Compliance-related incidents to highlight.

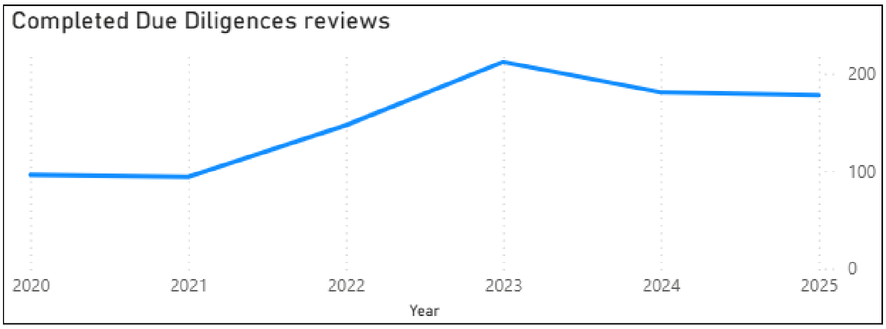
It should also be noted that Navantia monitors more than 800 companies included in the value chain through an alert system, in order to detect any incidents relating to corruption, the environment, labour matters, human rights and taxation.

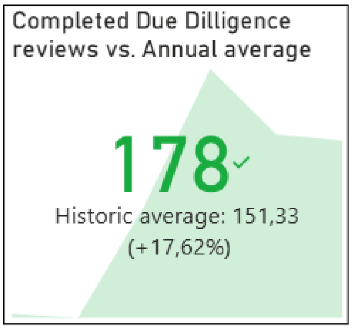
8.3. Total due diligence procedures performed

- **TYPE OF RELATIONSHIP**

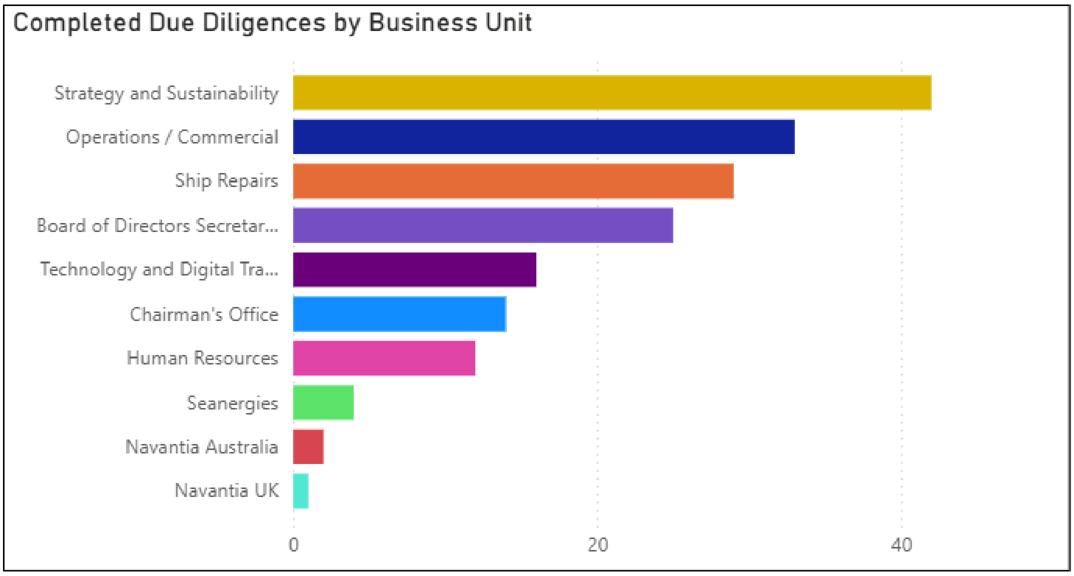


- **EVOLUTION OF DUE DILIGENCE REPORTS PREPARED OVER THE LAST 5 YEARS**

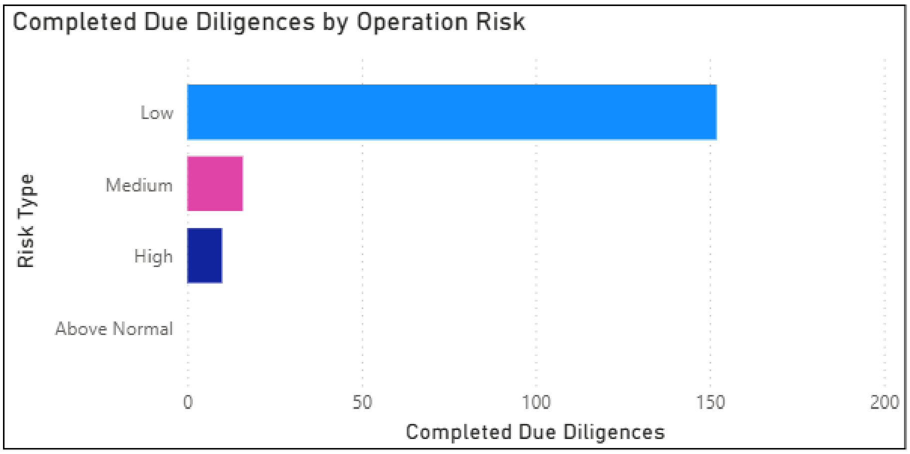




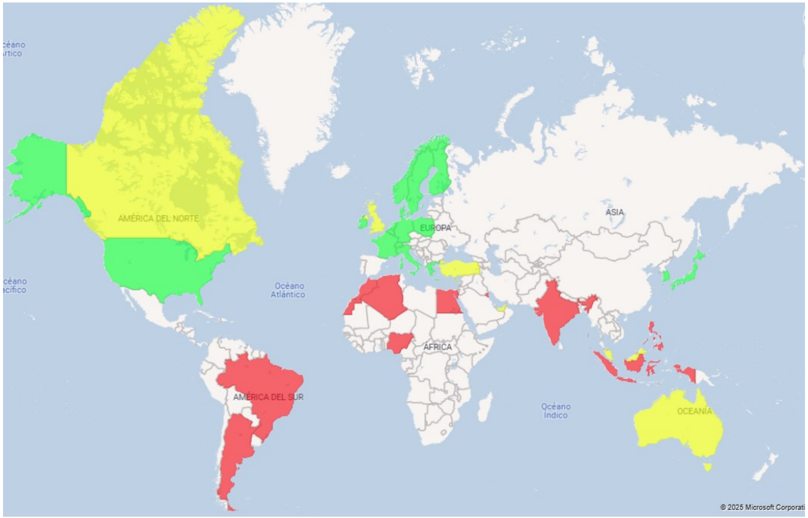
- **BY REQUESTING DEPARTMENT**



- **BY TYPE OF OPERATION RISK**



- **COUNTRY RISK OF THE OPERATION FOR COMPLIANCE PURPOSES (2025):**



9. ACTION PLAN MONITORING

9.1. Review of the map and reassessment of criminal risks

The main objective of the criminal risk assessment is to gain a better understanding of the organisation's exposure to such risks, so that Navantia can make more informed decisions regarding their management. This also enables the company to prioritise its risks and identify those that should be controlled first, drawing up an action plan and allocating the necessary resources for this purpose.

Through article 31 bis 5.1 of the Criminal Code, the Spanish legislator establishes that organisation and management models (Compliance) shall: "*1. identify the activities within the scope of which the offences to be prevented may be committed*".

The U.S. Federal Sentencing Guidelines state even more clearly that "*the organisation shall periodically assess the risk that criminal conduct will occur and shall take appropriate steps to reduce the risk of such criminal conduct*". They also state that the risk assessment should take into account "*the nature and seriousness of such criminal conduct*", "*the likelihood that certain criminal conduct may occur as a result of the nature of the organisation's business*" and "*the prior history of the organisation*".

In this regard, the Compliance Committee agreed to entrust the Compliance Department with the review of criminal risks, the result of which is attached as **Annex I**, after having been approved by the Compliance Committee.

9.2. Criminal risk controls

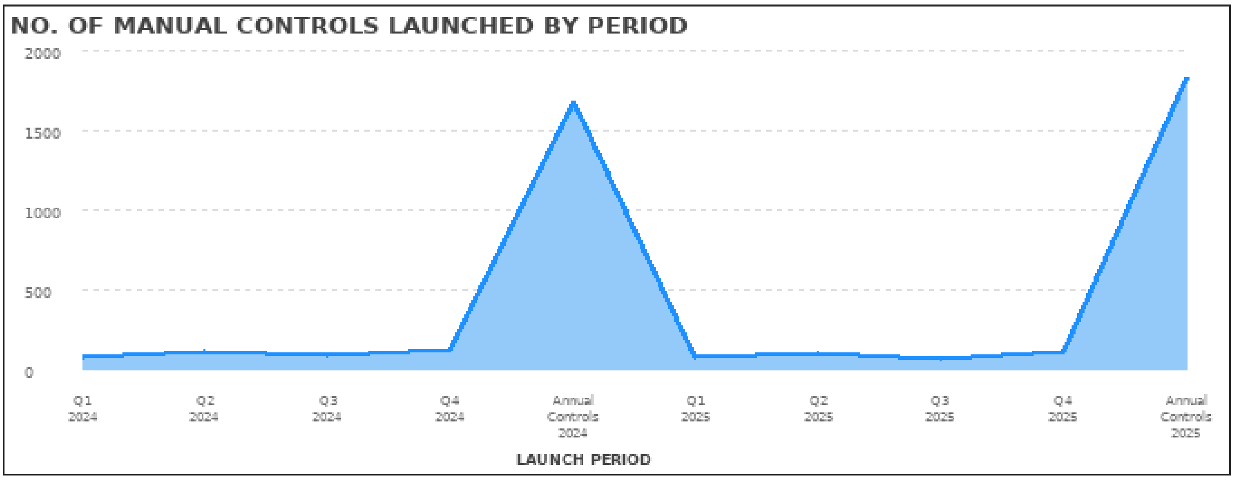
Control owners gain assurance regarding their controls by reporting incidents, doubts about the risks inherent to their specific activity or any other matter affecting them. For its part, through this type of ordinary communication, the prevention body can understand the evolution of the control system across the various procedures and, where appropriate, identify areas for improvement.

As a consequence of the reassessment of criminal risks, and as a result of both the regulatory updates carried out during the year and the adaptation to the new organisation defined within the company, it became necessary, as planned, to carry out an in-depth review of the controls defined in the company's various procedures, their adaptation to the new organisation and, finally, the identification of the new persons responsible for their execution and supervision.

This action, which is essential for controlling and mitigating the identified Compliance risks, was successfully completed during the year, incorporating the updated controls into the IT tool that facilitates their proper control and monitoring (SAP Governance Risk and Compliance (GRC)).

An indicator of the execution of GRC controls by the business owners (first line of defence) is attached:

- **Manual controls**



In total, during financial year 2025, 1,822 manual controls were launched, with a provisional annualised response rate of 53%. It should be noted that, at the date of issue of this Report, the fourth-quarter control cycle and the annual controls for 2025 are still being executed. This circumstance arose due to the following important matters:

- The technical incident preventing the execution of controls through interactive PDF documents has not been resolved; it has therefore been decided to abandon that method and controls will be executed by interacting directly in SAP GRC.

- The suitability of controls has been reviewed, discarding those that were obsolete or did not properly mitigate the identified risks.

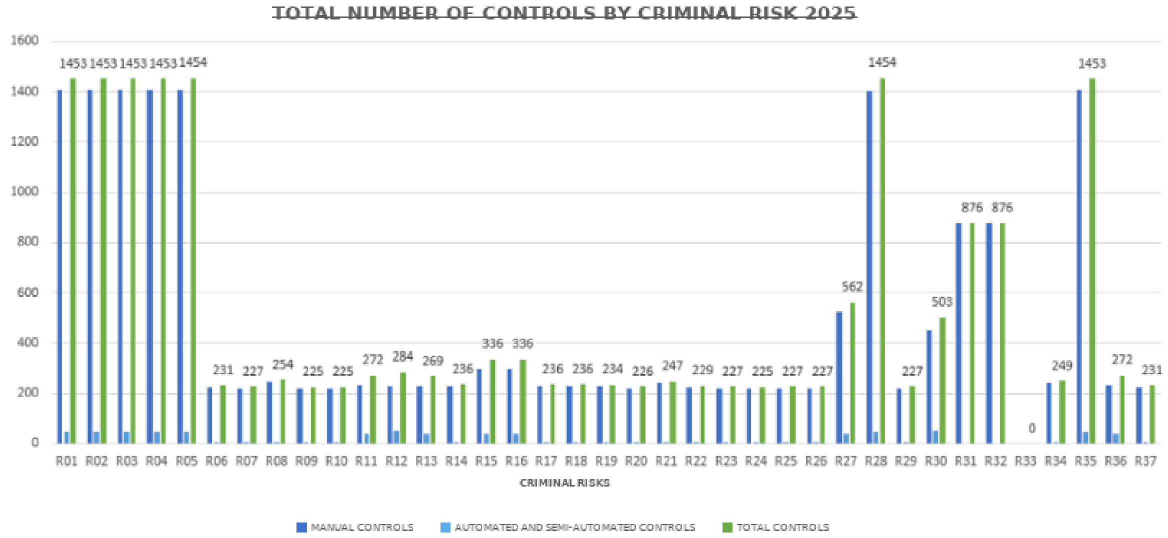
- The controls implemented in the Anti-Fraud System are incorporated in the testing phase.

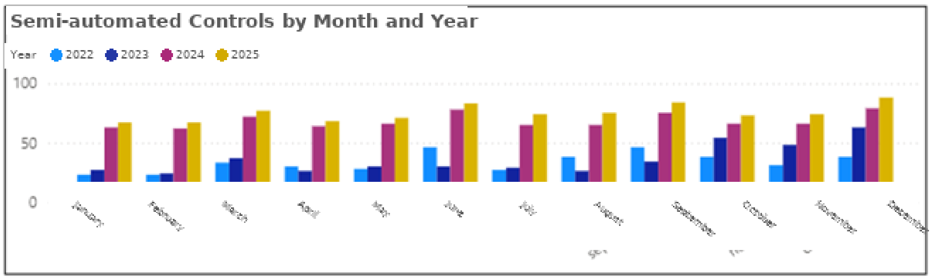
- **Semi-automatic controls**

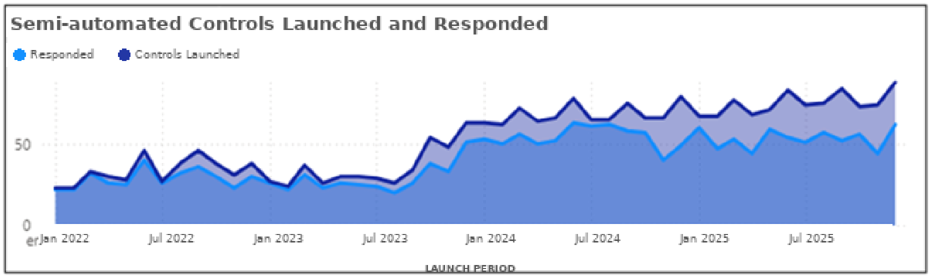
During financial year 2025, the semi-automatic controls were launched on a scheduled basis on the 22nd day of each month, corresponding to the data from the previous month and with a validity period of one month for their execution from the launch date. The system will automatically launch the SEMIA and AUTO controls relating to the data from the previous month/quarter/semester/year. The launches to date have been as follows:

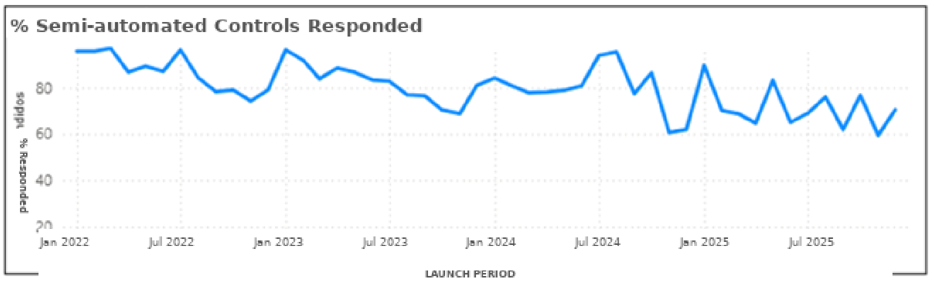
In total, 2425 controls were launched.

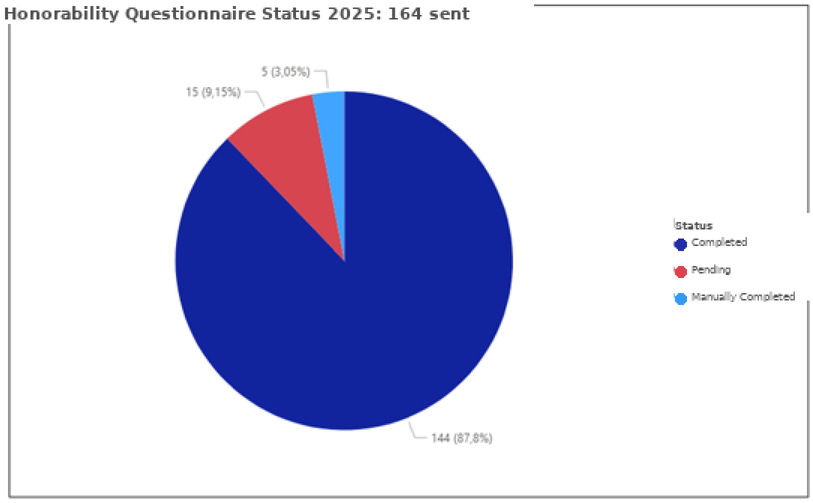
Below, we include tables showing the controls implemented for criminal risks.

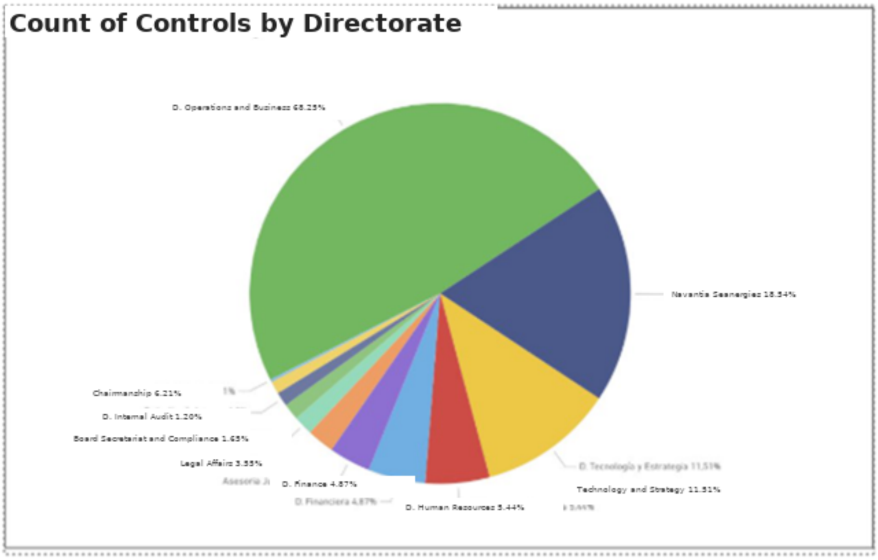












Directorate	Controls
D. Operations and Business	1170
D. Navantia Seanergies	450
D. Technology and Strategy	279
D. Human Resources	132
D. Finance	118
Legal Affairs	86
D. Sustainability and Continuous Im...	56
Board Secretariat and Compliance	40
Chairman's Office	34
D. Internal Audit	29
D. Systems and Services	26
Chairmanship	5
Total	**2425**

10. COMMITMENT

An ethical and compliance culture is essential in the business environment. It ensures that the organisation promotes behaviours that reinforce responsibility and transparency in all its operations, as well as ensuring compliance with applicable legal regulations. For this reason, ethics and corporate culture in compliance are fundamental to an effective and sustainable compliance model.

The development of a compliance culture requires the governing body and senior management to have a visible, consistent and sustained commitment over time to a common and published standard of behaviour required of each and every area of the organisation, as well as of its business partners.

In this regard, and as indicated above, Navantia has approved a Code of Conduct for Business Partners, such as customers, partners, suppliers, advisers and other related persons or entities. Acceptance of this Code by them is an essential requirement in order to establish business relationships with Navantia.

Internally within Navantia, the Compliance Department has requested acceptance of the integrity questionnaire addressed to persons who fall within any of the situations set out in Navantia's Anti-Corruption Procedure regarding due diligence on employees and executives, through the SAP GRC tool, with the following results:

As at the date of this report, work continues with the aim of obtaining acceptance of the integrity questionnaire by all employees.

11. GIFTS AND HOSPITALITY

Business courtesies, such as the giving of gifts and hospitality offered to or received from customers, suppliers and other partners, are a widespread practice in the business world to foster good relations and show recognition for professional dealings, with a number of common customs existing both as regards the type and value of the gift or invitation and the manner or protocol of exchange.

However, in some countries, no type of gift or invitation is permitted, as it is considered an act of bribery. Accordingly, business courtesies should not be offered without first reviewing the applicable anti-corruption legislation or being familiar with local customs.

Navantia

GIFT POLICY

Business courtesies, including gifts and hospitality offered to or received from customers, suppliers and other business partners, are common business practices intended to foster positive professional relationships and demonstrate appreciation for business interactions.

- Navantia has a catalogue of promotional and institutional gifts managed by General Services.
- Corporate credit cards may not be used to purchase gifts unless expressly authorized in accordance with internal procedures.
- Institutional gifts, awards, decorations, diplomas and similar recognitions that cannot be declined shall be accepted on behalf of Navantia and managed by General Services in accordance with company procedures.

SEE CORPORATE COMPLIANCE POLICY

*The gift policy is regulated in the P-CU-002 Anti-Corruption policy.

PROHIBITED GIFTS OR HOSPITALITY

- Cash or cash equivalents, including gift cards or vouchers.
- Gifts or hospitality prohibited by applicable laws or local regulations.
- Payments or benefits intended to obtain or retain contracts or to secure an improper advantage, such as favourable tax treatment.
- Gifts consisting of services or other non-cash benefits, such as an offer of employment.
- Any gift or hospitality offered during contract negotiations or a competitive tendering process.

ACCEPTABLE GIFTS OR HOSPITALITY

- Gifts or hospitality that do not create an expectation of preferential treatment or improper business advantages.
- Meals and refreshments consumed during a business marketing event.
- Business gifts with a maximum value of €50.
- Gifts and hospitality received or provided, provided the cumulative annual value from or to the same individual, company or organisation does not exceed €200. Where the annual threshold is exceeded, prior approval from the relevant manager and notification to the Compliance Department are required.
- Reasonable travel and accommodation expenses directly related to protocol, representation or legitimate business activities, subject to the required approvals.

KEY QUESTIONS BEFORE GIVING OR ACCEPTING A GIFT OR INVITATION

- Intention: What is the purpose of the gift or hospitality?
- Timing: Is it being offered during a contract negotiation, bidding process or important business decision?
- Audience: Am I attending alone or accompanied by other colleagues?
- Position: Is the recipient in a position to influence a decision related to Navantia?
- Context: Does this take place outside normal business circumstances?
- Frequency: Is this a recurring practice?
- Individualised: Is it intended for a specific individual rather than a broader group?
- Extent: Is it intended for me or also for my spouse, partner or family members?
- Public Disclosure Test: Would I feel comfortable if this gift or hospitality were publicly disclosed or reported in the media?

12. ETHICS CHANNEL

The prevention measures that make up the Compliance Management System cannot provide absolute protection against the commission of offences and, therefore, Navantia requires complementary systems that detect fraudulent behaviour in a timely manner.

To this end, Navantia has a communication channel through which employees, suppliers, agents, business partners and other third parties related to the company may report possible indications or incidents contrary to the law — whether criminal or administrative, of a serious or very serious nature— or to the conduct set out in Navantia's Business Code of Conduct.

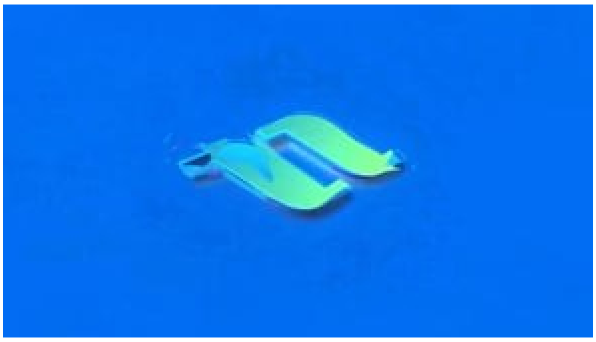
Through this Channel, Navantia complies with Law 2/2023 of 20 February, regulating the protection of persons who report regulatory breaches and the fight against corruption.

This mechanism is also available to receive enquiries regarding doubts that may arise in the application of the company's internal rules and procedures related to Regulatory Compliance.

12.1. Communication channels

The access channels to the Ethics Channel include, among others, the following:

- **Ethics Channel portal,** accessed through Navantia's website.
- **Telephone line:** +34 810 513 626
- **Email** addressed to: canaletico@navantia.es
- **Postal mail** addressed to:
  NAVANTIA, S.A., S.M.E. (**Compliance Department**)
  C/ Velázquez, 132, 28006
  Madrid (Spain)



12.2. Safeguards

- **Prohibition of retaliation:** no retaliation shall ever be taken against anyone who, in good faith, uses the Ethics Channel or cooperates in an investigation related to a possible breach of the Business Code of Conduct.

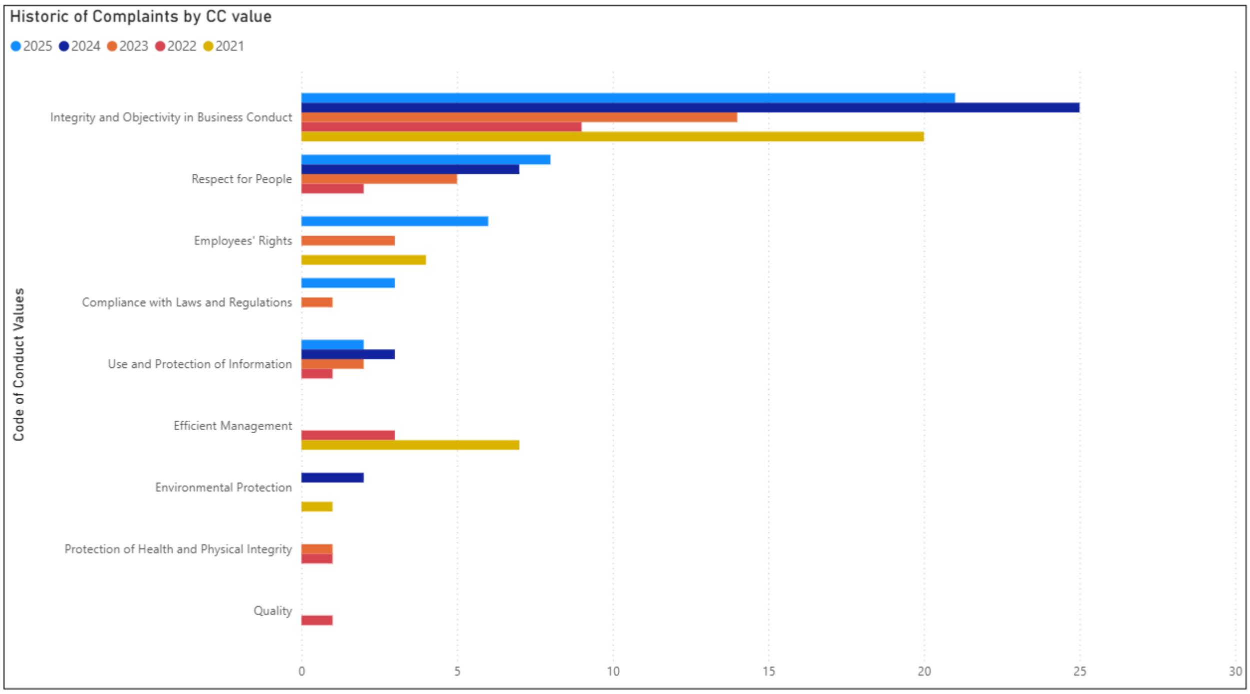
This safeguard does not apply to those who act in bad faith with the intention of disseminating false information or harming others. Navantia shall take any appropriate legal or disciplinary measures against such unlawful conduct.

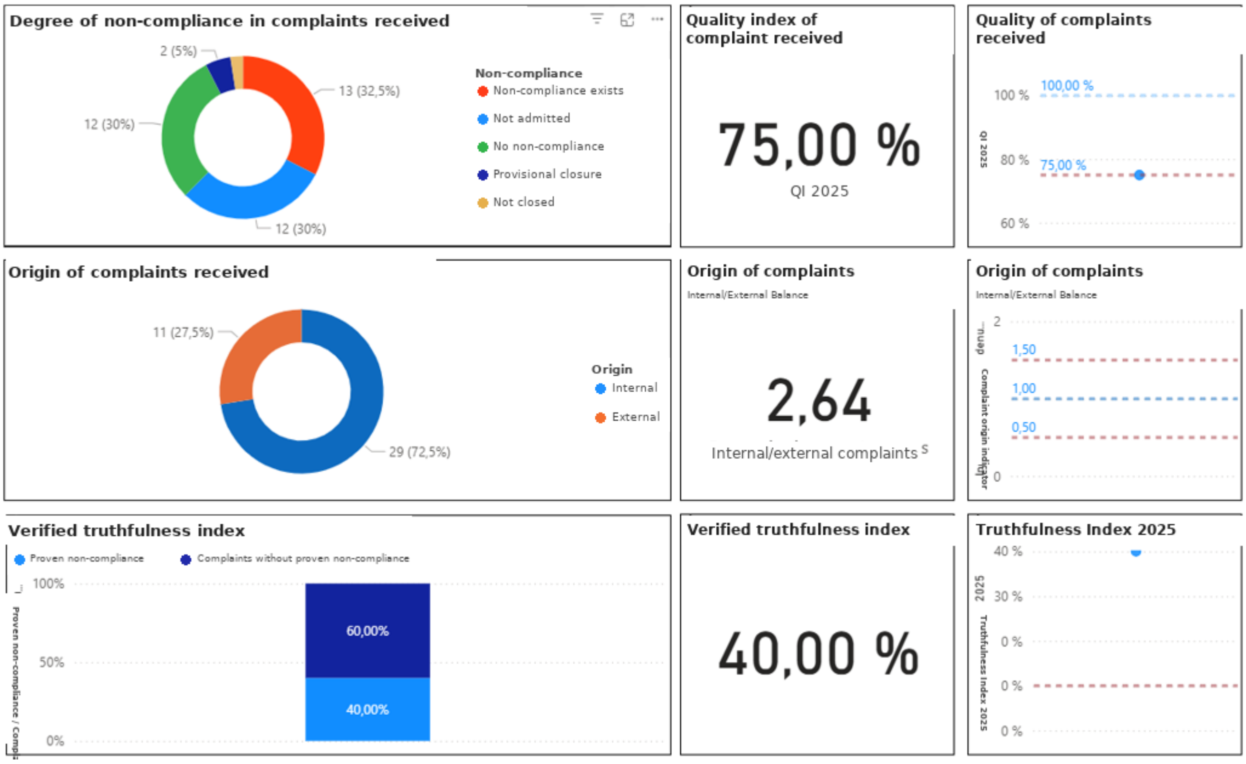
- **Confidentiality and anonymity:** reports may be submitted anonymously or with identification and, in either case, Navantia guarantees the confidentiality of the identity of the reporting person and of any third party mentioned in the report, as well as of the actions carried out in managing and processing it, together with data protection, preventing access by unauthorised personnel.

12.3. Reports received

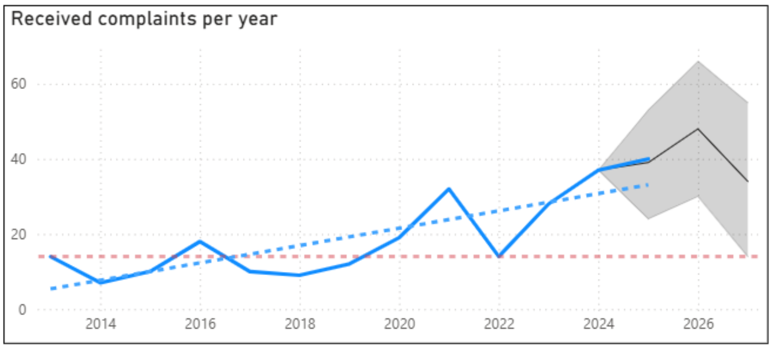
During financial year 2025, 40 reports were received.

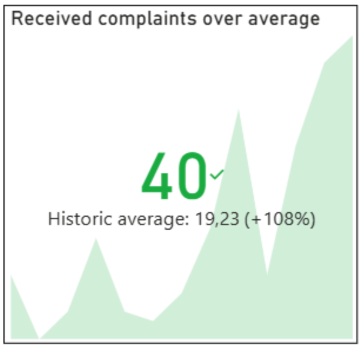
A chart is attached showing the distribution of reports received through the Ethics Channel during financial year 2025, according to the affected behaviour pattern (values of Navantia's Code of Conduct), the origin of the reports and their reliability.

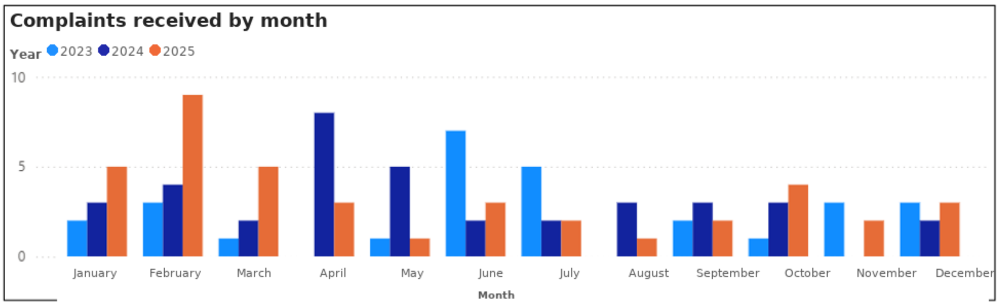




A chart is also included showing the evolution of the number of reports received through Navantia's Ethics Channel since it became operational in 2013, together with a monthly comparison of reports received in 2025.







12.4. Sanctions arising from Ethics Channel cases

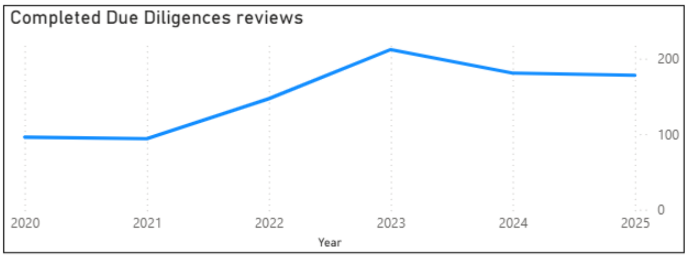
During financial year 2025, and as a result of cases managed through the Ethics Channel, 8 disciplinary proceedings were processed.

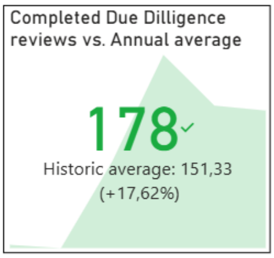
13. PERFORMANCE EVALUATION

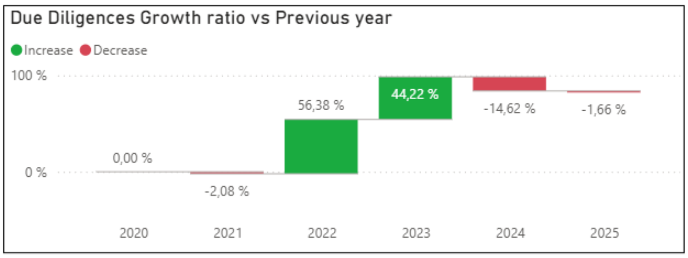
13.1. Indicators

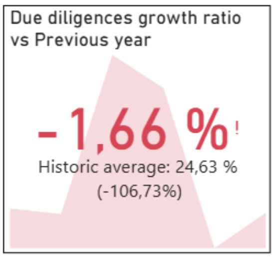
In order to assess the performance of the Compliance function, a series of KPIs have been established to objectively measure different key parameters in the various areas in which Compliance operates.

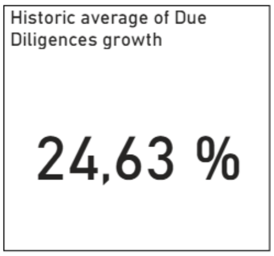
- **Due Diligence:** This measures the volume and annual growth of reviews and systematic analyses of the background of the entities with which Navantia maintains or plans to establish business relationships, ensuring that they comply with ethical and legal standards.



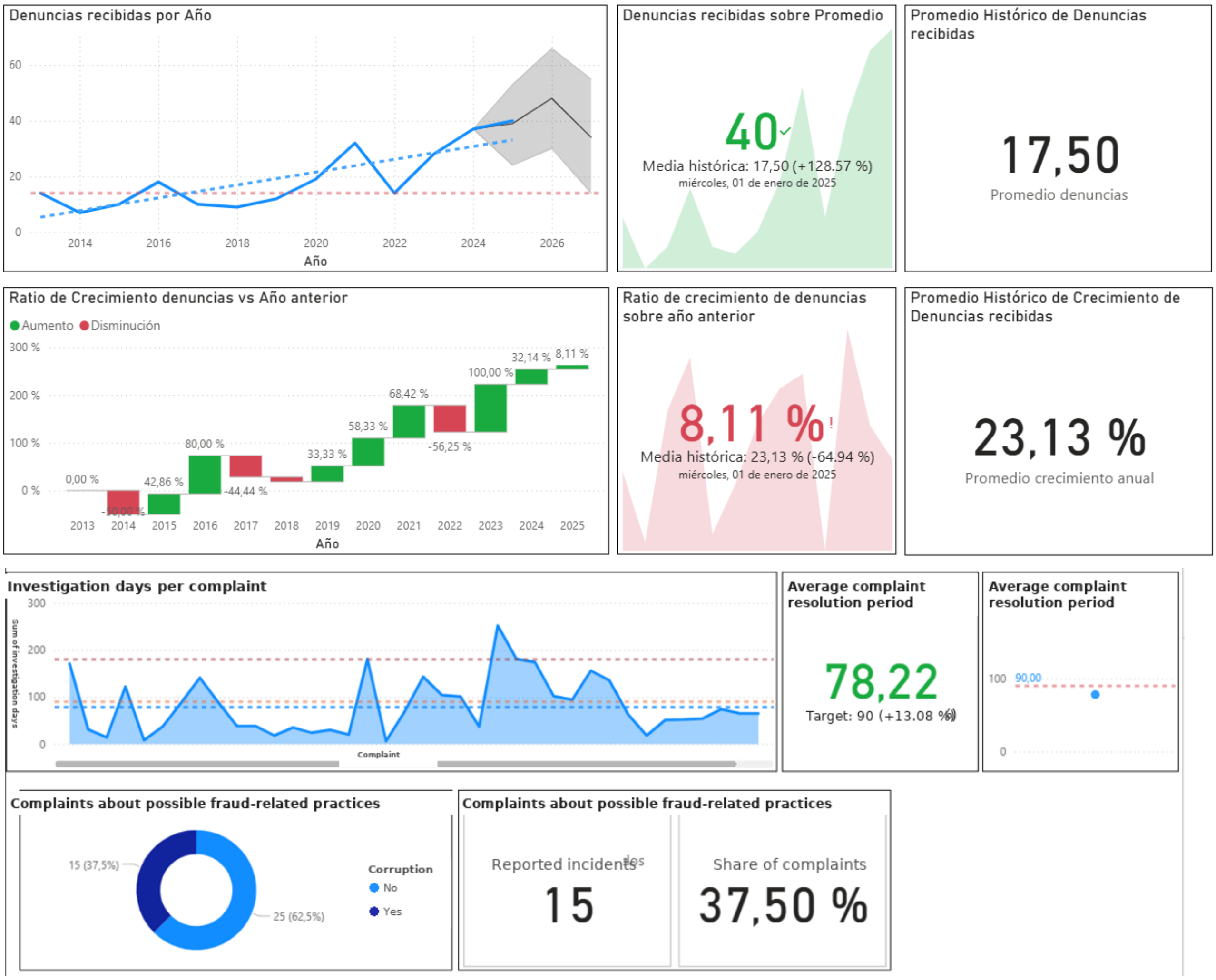








- **Ethics Channel:** This measures the number, type and origin of reports received through the Ethics Channel, as well as the response time for resolving each case.



13.2. Supplier evaluation survey

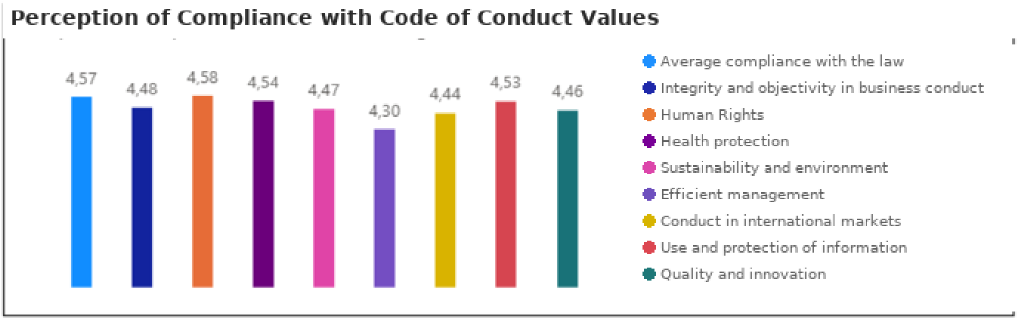
The Compliance Department carried out a performance evaluation survey on Compliance matters, addressed to all Navantia suppliers. This survey had a twofold objective: on the one hand, to obtain a realistic picture of the Compliance situation in the supply chain through a self-assessment process and, on the other hand, to obtain an assessment of Navantia's performance in Compliance aspects from the supply chain.

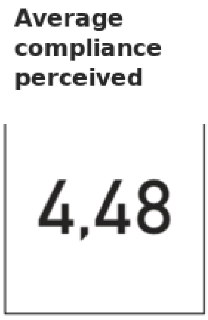
In collaboration with the Purchasing function, the survey was sent to a total of 3,486 suppliers (the study universe), obtaining a total of 818 responses, representing a 23.47% response rate.

Both objectives are expressed as an average score, obtained from the analysis and weighting of the responses received from each supplier. The supply chain self-assessment reached 49.54 out of 100, while Navantia's performance assessment obtained a score of 84.08 out of 100.

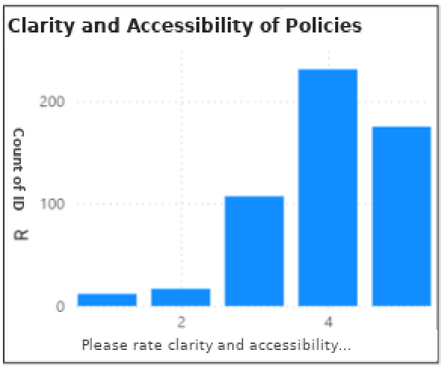
Within the supply chain self-assessment, it should be noted that 25.79% of respondents have the requirements and components of an approvable Management System, testing the existence of Anti-Corruption Policies, recent risk assessment, Ethics Channel/reporting channel, Conflict of Interest Management Procedures and Periodic Audits.

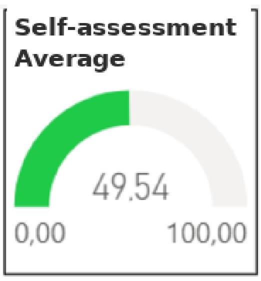
In the analysis of Navantia's Compliance performance, suppliers were asked to assess Navantia in relation to the different principles included in its Code of Conduct. The average score obtained was 4.48 out of 5, with "Efficient management" receiving the lowest score (4.30) and "Human rights" being the highest rated value (4.58).



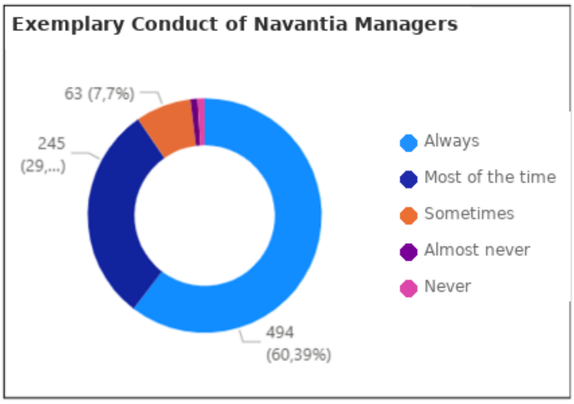


Likewise, respondents were asked to assess the clarity and accessibility of our policies, which obtained a score of 4 out of 5.





A subjective assessment was also requested regarding the exemplary conduct and commitment shown by Navantia's managers with respect to the principles of Navantia's Code of Conduct. The majority responses were "Always" and "Almost always" (90.34% in total), while "Never" and "Almost never" were marginal (1.96% in total).



As a result of the analysis of the survey results, the following conclusions should be highlighted:

- Navantia's perception in Compliance matters is very positive among suppliers, who particularly value the clarity, accessibility and example set by managers. However, there is room for improvement in communication and feedback regarding ethics channels and internal processes.

- The level of Compliance maturity in the supply chain is highly heterogeneous. While large companies and those with international certifications have solid and consolidated systems, a significant proportion of SMEs and micro-enterprises are at initial or intermediate stages of implementation, with barriers mainly associated with resources, time and knowledge.

- The main needs expressed by suppliers relate to training (basic and advanced), access to documentation and practical examples, support in certification processes and simplification of requirements and procedures.

- Improvement proposals for Navantia focus on strengthening communication and transparency, simplifying documentation and processes, improving the accessibility and feedback of the Ethics Channel, and offering practical training adapted to different supplier profiles.

14. SYSTEM AUDITS

14.1. Audits scheduled for the renewal of ISO 37001:2016 Anti-Bribery Management Systems certification

The **ISO 37001:2016** standard is the international anti-bribery management standard, and its main objective is to help companies combat bribery and promote an ethical business culture.

In 2019, the Compliance Committee decided to adopt ISO 37001:2016 as the standard for preventing, detecting and managing criminal bribery conduct, complying with legislation and other commitments voluntarily undertaken. Its most important characteristics are:

- The management system can be fully integrated with Compliance systems and other management systems, since the standard includes the common structure of ISO management system standards.

- The system is intended to prevent risks associated with bribery.

- It reflects international best practices and may be applied in any organisation, regardless of size, sector or country.

- It strengthens the organisation's reputation and integrity.

Accordingly, during financial year 2025, within the framework of the maintenance of ISO 37001:2016 Anti-Bribery Management Systems certification, Navantia was audited by the certification body **Bureau Veritas Iberia SL**.

- **External audit report on the maintenance of certification by Bureau Veritas Iberia SL (19577467) for "ISO 37001:2016"**

The report submitted by Bureau Veritas Iberia SL concludes that Navantia stands out for the high level of transparency of all its procedures, data, policies, etc., since much of this information is available on the website to all relevant stakeholders.

No "Non-Conformities" were detected during the audit. This audit was carried out between 1 and 12 December 2025.

	Major	Minor
Number of recorded Nonconformities	0	0

The following "strengths" were also highlighted:

5.4. STRENGHTS

- Variable compensation. Employee involvement in setting individual objectives
- Strong culture of compliance within the organization
- High level of commitment from Senior Management and the Compliance Committee

And, as an "Opportunity for Improvement", the following was identified:

5.5. OPPORTUNITIES FOR IMPROVEMENT

No.	Process	Opportunity for Improvement
1	CONTEXT – INTERESTED PARTIES	Identify the Independent Whistleblower Protection Authority as an interested party in the criminal compliance and anti-bribery management system.
2	CONTROLS	It is recommended to include a link or reference to the Ethics Channel as evidence of its dissemination and communication to third parties in the contractual clauses defined by the organization.
3	CONTROLS	Define a specific timeframe for deciding whether to submit the potential disqualification of a supplier to the Procurement Committee.
4	TRAINING	It is recommended that explicit reference be made to the Compliance Policy in the general training programme.
5	RISK ASSESSMENT	Clarify the historical sanctions criterion used to assess the likelihood of criminal and bribery risks.
6	RISK ASSESSMENT	Consider assessing those risks that the organization deems not applicable to Navantia's activities or alternatively indicate that general controls apply to them.

Thus, after successfully passing both audits, Navantia maintains its ISO 37001:2016 Anti-Bribery Management Systems certification.


Bureau Veritas Certification

Certificación

Concedida a

NAVANTIA S.A., S.M.E.

CL VELÁZQUEZ, 132 - 28006 - MADRID - ESPAÑA

Bureau Veritas Certification certifica que el Sistema de Gestión Antisoborno ha sido auditado y encontrado conforme con los requisitos de la norma:

NORMA

ISO 37001:2016

(UNE-ISO 37001:2017)

El Sistema de Gestión se aplica a:

DISEÑO, DESARROLLO, FABRICACIÓN/CONSTRUCCIÓN, MANTENIMIENTO Y APOYO AL CICLO DE VIDA DE BUQUES, SUBMARINOS, SISTEMAS Y OTROS PRODUCTOS DEL SECTOR NAVAL E INDUSTRIAL.

Número del Certificado:	ES141888 - 1
Aprobación original:	19-12-2023
Auditoría de certificación/renovación:	01-12-2023
Caducidad del ciclo anterior:	NA
Certificado en vigor:	19-12-2023
Caducidad del certificado:	18-12-2026

Este certificado está sujeto a los términos y condiciones generales y particulares de los servicios de certificación

Bureau Veritas Iberia S.L.
C/ Valportillo Primera 22-24, Edificio Caoba, 28108 Alcobendas - Madrid, España

ENAC CERTIFICACIÓN ISO 17021 Nº4 / C-SG105

1/2


Bureau Veritas Certification

Certification

Awarded to

NAVANTIA S.A., S.M.E.

CL VELÁZQUEZ, 132 - 28006 - MADRID - SPAIN

Bureau Veritas certification certifies that the Anti-bribery Management System has been audited and found to be in accordance with the requirements of standard:

STANDARD

ISO 37001:2016

(UNE-ISO 37001:2017)

Scope of certification:

DESIGN, DEVELOPMENT, MANUFACTURING/CONSTRUCTION, MAINTENANCE AND SUPPORT FOR THE LIFE CYCLE OF SHIPS, SUBMARINES, SYSTEMS AND OTHER PRODUCTS IN THE NAVAL AND INDUSTRIAL SECTOR.

Certificate Number:	ES141888 - 1
Original approval date:	19-12-2023
Certification/Renovation Audit:	01-12-2023
Expiry date of previous cycle:	NA
Effective date:	19-12-2023
Certificate expiration date:	18-12-2026

This certificate is valid, subject to the general and specific terms and conditions of certification services

Bureau Veritas Iberia S.L.
C/ Valportillo Primera 22-24, Edificio Caoba, 28108 Alcobendas - Madrid, España

ENAC CERTIFICACIÓN ISO 17021 Nº4 / C-SG105

1/2

14.2. Audit scheduled for obtaining UNE 19601:2017 Criminal Compliance Management System certification

UNE 19601:2017 establishes the requirements for implementing a Criminal Compliance Management System in public or private organisations. This Spanish standard was developed by the Spanish Association for Standardisation (UNE) as a reference framework to prevent offences, reduce criminal risks and promote an ethical corporate culture. It is directly aligned with the requirements of the Spanish Criminal Code, especially article 31 bis, which regulates the criminal liability of legal persons.

In 2024, the Compliance Committee decided to adopt UNE 19601:2017 as the standard to provide an effective framework for preventing and detecting offences within the organisation, mitigating or exempting the legal person from criminal liability and improving legal certainty, internal controls and the compliance culture. Its most important characteristics are:

- Risk-based approach: identifies and controls the organisation's relevant criminal risks.
- Senior management commitment: leadership and resources to promote a compliance culture.
- Controls and reporting channels: establishes preventive measures and a secure channel for reporting incidents.
- Supervision and continuous improvement: audits and periodic reviews to ensure ongoing effectiveness.

Accordingly, during financial year 2025, within the framework of obtaining UNE 19601:2017 Criminal Compliance certification, Navantia was audited by the certification body Bureau Veritas Iberia SL.

- **External audit report on obtaining certification by Bureau Veritas Iberia SL (28614257) for "UNE 19601:2017"**

The audit concludes that the Compliance Management System is fully aligned with the requirements of the standard and is properly implemented and maintained. It confirms that the policy commitments are integrated into the processes and that the system demonstrates maturity and effectiveness, with no non-conformities detected and only six opportunities for improvement. The system objectives are defined and monitored, and internal audits operate as an effective tool for continuous improvement. Management reviews and compliance body reviews confirm the proper operation of the system. Overall, the assessment is positive and the issuance of the new Criminal Compliance Management System certificate is recommended.

This audit was carried out between 1 and 12 December 2025:

	Major	Minor
Number of recorded Nonconformities	0	0

The following “strengths” were also highlighted:

5.4. STRENGHTS

- Variable compensation. Employee involvement in setting individual objectives
- Strong culture of compliance within the organization
- High level of commitment from Senior Management and the Compliance Committee

And, as “Opportunities for Improvement”, the following were identified:

5.5. OPPORTUNITIES FOR IMPROVEMENT

No.	Process	Opportunity for Improvement
1	CONTEXT – INTERESTED PARTIES	Identify the Independent Whistleblower Protection Authority as an interested party in the criminal compliance and anti-bribery management system.
2	CONTROLS	It is recommended to include a link or reference to the Ethics Channel as evidence of its dissemination and communication to third parties in the contractual clauses defined by the organization.
3	CONTROLS	Define a specific timeframe for deciding whether to submit the potential disqualification of a supplier to the Procurement Committee.
4	TRAINING	It is recommended that explicit reference be made to the Compliance Policy in the general training programme.
5	RISK ASSESSMENT	Clarify the historical sanctions criterion used to assess the likelihood of criminal and bribery risks.
6	RISK ASSESSMENT	Consider assessing those risks that the organization deems not applicable to Navantia’s activities or alternatively indicate that general controls apply to them.

Thus, after successfully passing both audits, Navantia has obtained UNE 19601:2017 Criminal Compliance Management System certification .

CERTIFICATE

Bureau Veritas Certification certifica que el Sistema de Gestión de

NAVANTIA SA, SME

CL VELÁZQUEZ, 132 - 28006 - MADRID - ESPAÑA

Este es un certificado con múltiples emplazamientos, los emplazamientos adicionales figuran en la(s) página(s) siguiente(s)

ha sido auditado y se encuentra conforme a los requisitos de la norma

Compliance penal UNE19601:2017

Alcance de certificación:

DISEÑO, DESARROLLO, FABRICACIÓN/CONSTRUCCIÓN, MANTENIMIENTO Y APOYO AL CICLO DE VIDA DE BUQUES, SUBMARINOS, SISTEMAS Y OTROS PRODUCTOS DEL SECTOR NAVAL E INDUSTRIAL.

Número de certificado: ES161542

Fecha de certificación original: 10-02-2026

Fecha de auditoría de certificación/recertificación: 04-12-2025

Fecha de caducidad del ciclo anterior: NA

Certificado en vigor: 10-02-2026

Caducidad del certificado: 09-02-2029

Versión Nº: 1

Este certificado está sujeto a los términos y condiciones generales y particulares de los servicios de certificación

Bureau Veritas Iberia S.L.
C/ Valportillo Primera 22-24, 28108 Alcobendas - Madrid, España

1/3

CERTIFICATE

NAVANTIA SA, SME

Compliance penal UNE19601:2017

Alcance de certificación:

Emplazamiento	Dirección	Alcance
NAVANTIA S.A., S.M.E. - MADRID	CL VELÁZQUEZ, 132 - 28006 - MADRID - ESPAÑA	DISEÑO, DESARROLLO, FABRICACIÓN/CONSTRUCCIÓN, MANTENIMIENTO Y APOYO AL CICLO DE VIDA DE BUQUES, SUBMARINOS, SISTEMAS Y OTROS PRODUCTOS DEL SECTOR NAVAL E INDUSTRIAL
NAVANTIA S.A., S.M.E. - PUERTO REAL	POLIGONO ASTILLERO, S/N - 11519 - PUERTO REAL - CADIZ - ESPAÑA	
NAVANTIA S.A., S.M.E. - CARTAGENA	CTRA. DE LA ALGAMECA, S/N - 30205 - CARTAGENA - MURCIA - ESPAÑA	
NAVANTIA S.A., S.M.E. - PERLIO-FENE	CTRA. DE LA RIBERA, S/N - 15500 - PERLIO-FENE - A CORUÑA - ESPAÑA	
NAVANTIA S.A., S.M.E. - SAN FERNANDO	CTRA. DE LA CARRACA, S/N - 11100 - SAN FERNANDO - CADIZ - ESPAÑA	
NAVANTIA SA, SME - FENE	AVDA. DAS PIAS, S/N - 15500 - FENE - A CORUÑA - ESPAÑA	
NAVANTIA SA, SME - CADIZ	CTRA. INDUSTRIAL, S/N - 11005 - CADIZ - ESPAÑA	

Número de certificado: ES161542

Versión Nº: 1

Este certificado está sujeto a los términos y condiciones generales y particulares de los servicios de certificación

Bureau Veritas Iberia S.L.
C/ Valportillo Primera 22-24, 28108 Alcobendas - Madrid, España

2/3

14.3. Audit of compliance with Law 2/2023 - SEPI

SEPI's 2024 Annual Internal Audit Plan included, as an action to be carried out at Navantia, the verification of compliance with Law 2/2023 of 20 February, regulating the protection of persons who report regulatory breaches and the fight against corruption.

The following recommendations detailed in that report were mentioned for Navantia:

VII. RECOMMENDATIONS

FIRST (HIGH PRIORITY). - mprove NAVANTIA's Information Management Procedure in the following areas:

- **(R.1.1)** Include the deletion of reports containing special categories of personal data and false information within the timeframes established in Law 2/2023.
- **(R.1.2)** Include a specific section providing more detailed information on the management and protection of personal data within the Internal Information System.
- **(R.1.3)** Assess the possibility of extending the two-year protection period established in Law 2/2023 in order to strengthen measures against potential retaliation directed at reporting persons.

SECOND (MEDIUM PRIORITY).- Improve the electronic information reporting tool in the following areas:

- **(R.2.1)** Communication Receipt: The tool should allow anonymous reporting persons to receive acknowledgements of receipt and other communications without the need to provide an email address or telephone number, for example through the generation of a random user code and password.

- **(R.2.2)** Conflict of Interest: The tool should provide reporting persons with the option to change the recipient of the report, allowing them to select an alternative recipient if they believe that an actual or perceived conflict of interest exists.
- **(R.2.3)** Confidentiality: The tool should be certified under the Spanish National Security Framework (ENS) at least at the Medium level.
- **(R.2.4)** Data Centralization: Assess the use of a tool that consolidates all information related to reports and their handling, thereby avoiding the current multiplicity of systems (web forms, email, Microsoft Teams, shared folders) with the aim of reducing the risk of unauthorized access and improving confidentiality and data protection.

THIRD (MEDIUM PRIORITY)

- **R.3.1)** Obtain NAVANTIA's National Security Framework (ENS) Certificate of Conformity.
- **(R.3.2)** Should the tool be procured from an external third party in the future, the successful bidder must provide an ENS Certificate of Conformity at least at the Medium category level. In addition, the information system hosting the IT tool (internal reporting channel) must also be certified.

FOURTH (Medium Priority). - (R.4) In cases where the three-month period for completing investigations is exceeded due to the complexity of the investigation or exceptional circumstances, the reasons for the delay should be documented.

FIFTH (High Priority). - (R.5) Assess reducing the number of users with access to the Internal Information System, both from a confidentiality and personal data protection perspective.

SIXTH (High Priority). - (R.6) Conduct training initiatives for all employees to ensure they are adequately informed about the Ethics Channel and about the obligation to report communications received through unauthorized channels to the person responsible for the Internal Information System, in accordance with Article 9.2(g) of **Law 2/2023**.

SEVENTH (Medium Priority). - (R.7) Implement a secure long-term retention system for closed case files (i.e., cases where the internal investigation phase has been completed) to ensure confidentiality and information recoverability, eliminating the use of encrypted USB drives stored in a safe.

EIGHTH (Medium Priority). - (R.8) Extend the scope of this audit to NAVANTIA subsidiaries so that the entire NAVANTIA Group is subject to a consistent and harmonized approach in this area.

Navantia's Internal Audit Department, together with SEPI's Internal Audit Department, is responsible for monitoring the recommendations. Although the audit was carried out in the previous financial year, 2024, during financial year 2025 the recommendations indicated by SEPI have continued to be implemented on an ongoing basis.

As at the date of this report, almost all the recommendations have already been fulfilled, with the exception of one. Among those fulfilled are the obtaining of the National Security Scheme certificate, improvements to the Ethics Channel tool to acknowledge receipt, report on the status of cases, optimise the conflict-of-interest reporting tool, generate a code for registering incidents in the Ethics Channel and ensure anonymity, improve the reporting and control of investee companies (subsidiaries), etc.

15. CONTINUOUS IMPROVEMENT. 2026 OBJECTIVES

As part of its continuous development, the Compliance Committee agreed on the following objectives for the Compliance Department for financial year 2026:

- Implement the 4th phase of Navantia's Internal Fraud Prevention and Detection System and submit its results to the Compliance Committee for monitoring.
- Define and implement a dashboard for the Anti-Fraud System, enabling the governing bodies to carry out the supervision and verification functions provided for in the Compliance Committee Regulations.
- Implement a systematic model for managing Compliance due diligence risks linked to ISO 37001 and UNE 19601 standards, applicable to strategic partners and collaborators.
- Reassess the criminal risk and control matrix in Compliance matters linked to ISO 37001 and UNE 19601 standards.
- Implement the actions arising from the ISO 37001, UNE 19601 and SEPI audits (Ethics Channel) in order to ensure compliance.

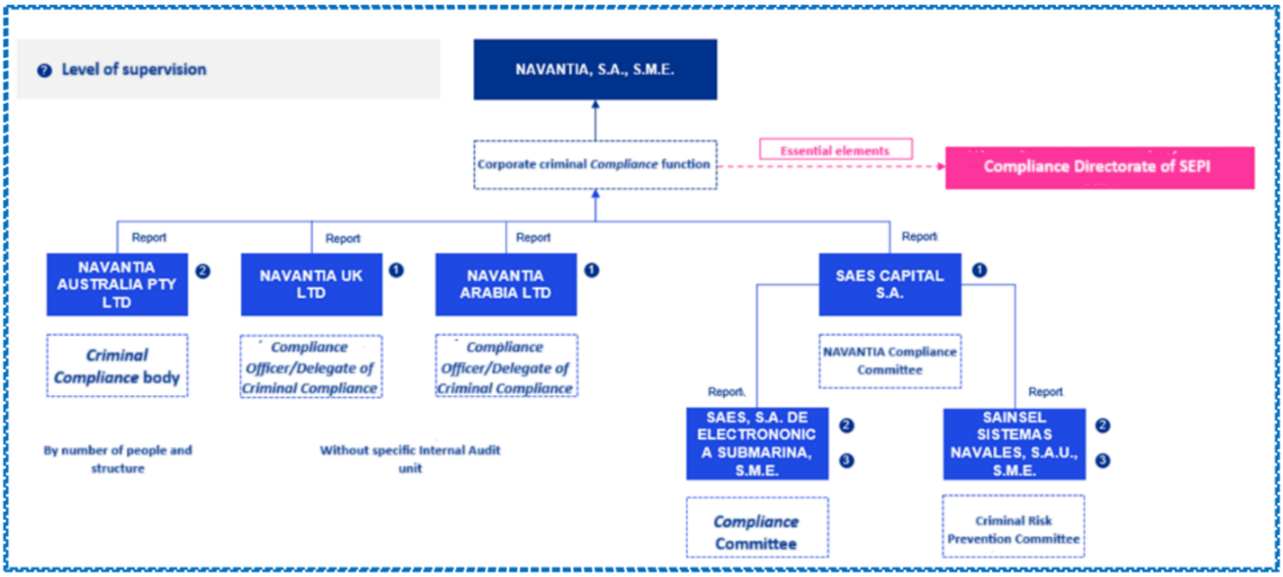
After approval by the Compliance Committee, the proposed objectives are reported to the Board of Directors.

The actions arising from these objectives will be developed by the Compliance Department, and their level of completion will be reported periodically to the Compliance Committee, the Management Committee and the Board of Directors.

16. NAVANTIA GROUP COMPLIANCE SYSTEM

During financial year 2025, the Compliance Supervision and Reporting System of the Navantia Group was effectively deployed. This system is based on the existence of three levels of supervision, defined according to the maturity level of the subsidiaries' control bodies:

- Supervision level **1**: Navantia's Criminal Compliance Function assumes Criminal Compliance activities for controlled investees — CENTRALISED.
- Supervision level 2: Navantia's Criminal Compliance Function issues guidelines for controlled investees and supervises their implementation — CENTRALISED HYBRID.
- Supervision level 3: Navantia's Criminal Compliance Function issues guidelines to controlled entities and is informed — DECENTRALISED HYBRID.



The deployment was carried out according to the type of shareholding and the maturity level of the local Compliance systems. The objective was to strengthen traceability, model consistency and monitoring capacity at Group level.

In **controlled companies**, a gradual deployment by supervision levels (1–3) was applied, combining formal communications to senior managers with coordination meetings with local Compliance functions where necessary. Formal requests for evidence were made, and supporting system documentation was received and reviewed, including, among others, elements of the Internal Reporting System, channel documentation and its register book, risk maps, and training and awareness plans. Periodic submission guidelines and prior communication of changes to essential elements were established in accordance with P-CU-006. In subsidiaries without a fully operational proprietary system (Navantia UK and Navantia Arabia), Navantia temporarily assumed the Compliance function and channel management, while also promoting the preparation/adaptation of the applicable regulatory framework and the allocation of resources for its progressive implementation.

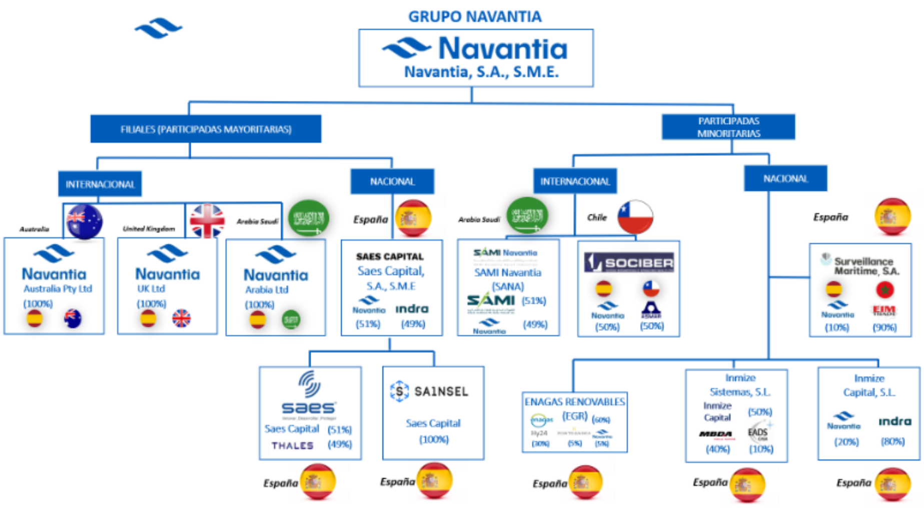
In **non-controlled companies**, and taking into account the limitations arising from their integration into other corporate groups, a coordination scheme was established with the directors appointed by Navantia in order to channel requests for information on local compliance systems, provide a prior advisory channel for decisions and promote continuous improvement initiatives within the available sphere of influence.

The progress of the actions and the execution status of the Plan were reported to the Compliance Committee, strengthening accountability and monitoring of the model. In addition, the corresponding closing communication was made together with the submission of the associated documentation.

17. REPORTING BY NAVANTIA GROUP SUBSIDIARIES ON THEIR COMPLIANCE SYSTEM

This section summarises the Compliance-related activities of the investee companies, with the aim of informing Navantia’s governing body of the degree of implementation and operation of their criminal and corruption risk models.

This reporting, adapted to the requirements of international standards, takes the form of the submission of a report on Compliance activities prior to its approval by the corresponding governing body of each company.



17.1. INTERNATIONAL MAJORITY-OWNED INVESTEES

- **Navantia Australia Pty Ltd. (NAVANTIA AUSTRALIA)**

Navantia Australia, through its chair, submitted the Compliance activities report for financial year 2025.

This report includes, among other aspects, the meetings of the Compliance Committee, regulatory amendments, due diligence procedures carried out, organisational changes, monitoring and updating of risks and controls, Compliance training actions and the budget for financial year 2025.

During 2025, improvements were implemented in the deployment of training, compliance with requirements by suppliers, reporting in SAP GRC and the strengthening of the Compliance Management System. Thanks to the leadership and involvement of Navantia Australia's governing bodies, visibility has increased in order to define Compliance objectives and actions that help strengthen risk management and compliance in relation to criminal risks.

The most noteworthy aspects implemented during this period were:

- **Training**
  - Navantia Australia: *Respect at Work*
  - Navantia Australia: *Psychosocial Hazards*
  - *Building Respectful Relationships*
  - Compliance Framework refresher training.
- **Risk management**

  Incorporation of new risks and updating of controls in accordance with Predict's Risk Management Model 6.4.1.

- **Governance reporting**
  - Compliance with the reporting requirements of the Attorney-General's Department (Commonwealth of Australia) under the *Modern Slavery Act*.
  - Certificate of compliance with the *Workplace Gender Equality Act 2012*.

It was also indicated that no reports had been received through the Ethics Channel.

- **NAVANTIA ARABIA Ltd. and NAVANTIA UK Ltd.**

Not applicable. They do not have their own Compliance Management Model or System, and the Compliance functions are assumed by Navantia's Compliance Committee.

The activities carried out in these companies during 2025 are included in section 17 of this report, concerning the reporting by Navantia Group subsidiaries on their Compliance system.

17.2. NATIONAL MAJORITY-OWNED INVESTEES

- **SAES CAPITAL**

SAES CAPITAL is a holding or capital company, carrying out, in whole or in part, the activities included in its corporate purpose indirectly through ownership of the shares of SAINSEL (100%) and SAES (51%).

- **SAES**

SAES's Board of Directors, through its Compliance Officer, submitted the Compliance activities report for financial year 2025.

This report details, among other matters, the meetings of the Compliance Committee, regulatory amendments, due diligence procedures carried out, organisational changes, monitoring and updating of risks and controls, Compliance training actions and the budget for financial year 2025.

As an annual review for financial year 2025, Navantia's Internal Audit area carried out an audit of SAES's Management System. This process has strengthened visibility over the different control areas, facilitating the identification of risks and the definition of objectives and actions aimed at the continuous improvement of the system and greater control of corporate risk.

For the proper execution of this audit, work was carried out continuously over several months with Navantia's auditors, to whom all required documentation was provided, while queries and requests for information made within the audit process were also addressed in a timely manner.

Likewise, the Compliance Committee met a total of 10 times during the year in order to analyse and approve the mandatory reports relating, among other matters, to the engagement of agents, SAES's participation in consortia and the Corporate Social Responsibility (CSR) Plan prepared during the year covered by this report.

In addition, the Support Unit was convened and met, and the functions entrusted to it within the Compliance system were presented and clarified. In this context, the corresponding documentation was delivered, systematically recording the controls carried out during financial year 2025.

Finally, during financial year 2025, 2 reports were received.

- **SAINSEL**

SAINSEL's Board of Directors, through its Compliance Officer, submitted the Compliance activities report for financial year 2025.

SAINSEL's Compliance report provides information on the review of the regulatory system, the activity of the Compliance body, the due diligence procedures carried out, organisational changes, the reassessment and monitoring of risks and controls, Compliance training actions and the activity plan for financial year 2025, among other matters.

Likewise, during 2025, two reports were received through the reporting channel (canaldenuncia@sainsel.es).

During 2025, two audits relating to the crime prevention model of SAES and SAINSEL were included in the Internal Audit Plan. The audit work relating to SAES's crime prevention model has been completed and the final report has been issued.

With regard to the subsidiary SAINSEL, this company was subject to an operational and compliance audit by the IGAE, with the final report issued on 2 October 2025. This report warned of risks of non-compliance in personnel matters and also in procurement management. Taking into account the conclusions issued by the IGAE, which have been supplemented by a procurement management audit carried out by Navantia's Internal Audit Department (DAI), as well as the company's own risk analysis and the resources available to Navantia's DAI, it was considered more appropriate to include, in the proposals for the 2026 Internal Audit Plan submitted to SEPI's Internal Audit Department, an action entitled "Monitoring of SAINSEL Actions: procurement management and control", and also to monitor the actions carried out by the subsidiary to comply with the IGAE recommendations, rather than carrying out an audit of the crime prevention model at this time.

Taking into account these actions and the time required to fully implement the measure relating to SAINSEL, this recommendation can only be considered partially fulfilled, with the expected completion date extended to 2027.

18. TRANSPARENCY OBLIGATIONS

18.1. Active disclosure obligations

Navantia complies with the active disclosure obligations imposed on it by Law 19/2013 of 9 December on transparency, access to public information and good governance (LTBAIG), through its Transparency Portal, publishing its organisational, economic, budget planning and statistical information.

In the latest assessment carried out by the Council for Transparency and Good Governance (CTBG), which included Navantia, compliance with active disclosure obligations was analysed for 75 entities belonging to the Institutional Public Sector. The CTBG awarded Navantia a score of 96.7% in the Mandatory Information Compliance Index (ICIO), making it the fourth most transparent company in terms of active disclosure across the Spanish public sector.

Since that assessment, Navantia has continued working to further increase transparency.

	Content	Format	Structure	Accessibility	Clarity	Reuse	Update	Total
Institutional, organisational and planning information	91,7	100,0	100,0	100,0	100,0	100,0	83,3	96,4
Economic, budgetary and statistical information	100,0	88,9	100,0	88,9	100,0	88,9	100,0	95,2
Mandatory Information Compliance Index	***96,7***	***93,3***	***100,0***	***93,3***	***100,0***	***93,3***	***93,3***	***96,7***

18.2. Access obligations

In compliance with the LTBAIG, Navantia promotes the exercise of the right of access by all citizens, providing them with public information held by Navantia, subject to the exceptions established by law and guaranteeing the rights of the affected persons, in particular their fundamental right to data protection.

The procedure for exercising this right of access shall begin with the submission of the corresponding request addressed to Navantia through one of the following channels:

- **Postal mail**: Navantia, S.A. S.M.E. Calle Velázquez 132, 28006 Madrid
- **Email:** buzontransparencia@navantia.es
- Through the **Transparency Information Unit** of the Ministry of Finance

The above information is set out in detail in the "Transparency Mailbox" section of Navantia's Transparency Portal.

In 2025, a total of 12 requests for the exercise of the right of access were processed.

CASE FILE	SUBJECT OF THE REQUEST	CHANNEL THROUGH WHICH THE INFORMATION REQUEST WAS RECEIVED	OUTCOME OF THE DECISION	RESOLVED WITHIN THE DEADLINE	APPEAL BEFORE THE TRANSPARENCY COUNCIL	OUTCOME OF THE TRANSPARENCY COUNCIL DECISION
2025-0001	Information on the number of Christmas hampers purchased in 2024, unit cost, total cost, their contents and whether they form part of the Christmas bonus salary payment. If there are several types of Christmas hamper, the unit cost and contents of each type are requested. List of senior officials who received them and the type of hamper received.	Transparency Portal of the Ministry of Finance	Granted	Yes	No	N/A
2025-0002	Information relating to the declaration of exceptionality regarding compliance with the reserved quota for workers with disabilities.	Navantia Transparency Portal	Granted	Yes	No	N/A
2025-0003	Access to statistics on the number of women and men employed by Navantia from 1900 to the present.	Navantia Transparency Portal	Rejected as inadmissible	Yes	No	N/A
2025-0004	Access to specific information related to procurement file MAD-2025-01-13 Special SBTi Advisory Services (51-31799). Specifically: a) Financial bids submitted by the bidding companies. b) Technical evaluation of the proposals and scores obtained, both by the requesting company and by the other bidding companies.	Navantia Transparency Portal	Granted	Yes	No	N/A
2025-0005	Information on the number of vessels built by Navantia for the Royal Moroccan Navy between 2010 and 2025.	Transparency Portal of the Ministry of Finance	Granted	Yes	No	N/A
2025-0006	Detailed information on the expenses incurred by Navantia for the CANSEC 2025 event in Ottawa.	Transparency Portal of the Ministry of Finance	Granted	Yes	No	N/A

2025-0007	Information related to employee absenteeism.	Transparency Portal of the Ministry of Finance	Partially granted	Yes	No	N/A
2025-0008	Information on the number of Hikvision cameras installed in Navantia facilities, as well as those still pending installation. In addition, the total expenditure on these cameras and their installation, broken down by year.	Transparency Portal of the Ministry of Finance	Granted	Yes	No	N/A
2025-0009	Information on administrative review procedures and claims for financial liability during the period 2023–2025.	Transparency Portal of the Ministry of Finance	Granted	Yes	No	N/A
2025-0010	Information on the cost of Navantia's counter-drone unit and its use.	Navantia Transparency Portal	Partially granted	Yes	No	N/A
2025-0011	List of Communications Directors and their remuneration in the following public companies: Adif, Aena, Correos, Loterías y Apuestas del Estado, RTVE, EFE, Navantia and SEPI.	Transparency Portal of the Ministry of Finance	Granted	Yes	No	N/A
2025-0012	Number of reported cases of sexual harassment and gender-based harassment between June 2018 and March 2024, indicating whether each complaint was upheld or dismissed, as well as the measures adopted against the offender in substantiated cases (fines, disciplinary sanctions, dismissals, etc.).	Transparency Portal of the Ministry of Finance	Granted	Yes	No	N/A

ANNEX I Criminal Risk Reassessment

Criminal Risk Catalogue

Reference	Criminal Risk Inventory
R.1 | R.2 | R.3 | R.4	Public Corruption (*) | Illegal Financing of Political Parties
R.5	Bribery in Business
R.6	Fraud
R.7	Misleading Advertising
R.8	Breach of Trade Secrets
R.9 | R.10	Subsidy Fraud | Fraudulent Obtaining of European Union Funds
R.11	Tax Fraud
R.12	Social Security Fraud
R.13	Non-Compliance with and Falsification of Accounting Obligations
R.14	Offences Against Natural Resources and the Environment
R.15 | R.16	Punishable Insolvency | Obstruction of Enforcement Proceedings
R.17 | R.18	Offences Relating to Intellectual and Industrial Property
R.19	Cybercrime
R.20	Urban Planning Offences
R.21	Offences Against Personal and Family Privacy
R.22	Offences Relating to Ionising Radiation
R.23	Offences Creating Risks Through Explosives and Other Hazardous Agents
R.24	Offences Against the Rights of Foreign Nationals
R.25	Public Health Offences
R.26	Smuggling
R.27	Money Laundering and Terrorist Financing (**)
R.28	Misappropriation of Public Funds
R.29	Bid Rigging and Manipulation of Prices in Public Tenders and Auctions (***)
R.30	Offences Against Workers' Rights (***)
R.31 | R.32	Offences Against Moral Integrity (Degrading Treatment) and Sexual Freedom
R.33	Animal Welfare Offences
R.34	Disclosure of Secrets Related to National Defence (****)
R.35	UK Bribery Act 2010 (*****)
R.36	Facilitating UK and Foreign Tax Evasion (*****)
R.37	Failure to Prevent Fraud Offence (*****)

(*) Public Corruption includes the following criminal risks: bribery, influence peddling, and corruption of public officials or authorities in international business transactions (see the *"Identified Risks"* tab).

(**) The identification of potential economic offences may also imply the existence of a criminal risk relating to money laundering and terrorist financing.

(***) Offences that may give rise to specific penalties pursuant to Article 129 of the Spanish Criminal Code.

(****) Offences which, while not giving rise to corporate criminal liability under the Spanish Criminal Code, are of particular relevance in light of NAVANTIA's corporate purpose and activities.

(*****) UK corporate offences.

INHERENT RISK:

To allocate resources efficiently and effectively to the risks identified in the various activities/processes/areas of a company, a good practice is to classify both the **likelihood of occurrence** and the **potential impact of such occurrence**.

Impact x Likelihood = **Risk**

Impact: The extent of the damage that the materialisation of a risk into an actual event would cause to the achievement of Navantia's objectives. It is assessed on a scale from 0 to 5.

IMPACT		
ASSESSMENT	COMPLIANCE AND CRIMINAL	REPUTATIONAL
1 POINT - VERY LOW	Administrative sanction or conviction imposing a daily-rate or proportional fine that does not cause the company to experience liquidity tensions within a period not exceeding one month.	Occurrence of an isolated event that does not reach the market.
2 POINTS - LOW	Administrative sanction or conviction imposing a daily-rate or proportional fine that requires the company to adopt mitigation actions that do not go beyond the scope of the Corporate Directorate.	Occurrence of an event that reaches stakeholder groups or appears in local media.
3 POINTS - MEDIUM	Administrative sanction or conviction imposing a daily-rate or proportional fine that requires the company to obtain additional financing from shareholder resources.	Occurrence of an event that reaches stakeholder groups or appears on the inside pages of relevant national media.
4 POINTS - HIGH	Conviction imposing a daily-rate or proportional fine that places the company in a situation requiring share capital reduction, disqualification from obtaining public aid or benefits and tax incentives, or temporary prohibition from carrying out certain activities in whose exercise the offence was committed.	Loss of reputation due to various actions or events affecting the image and appearing on the first inside pages of relevant national media.
5 POINTS - VERY HIGH	Conviction imposing a daily-rate or proportional fine that places the company in a situation requiring dissolution; dissolution of the legal entity; suspension of activity or closure of premises (max. 5 years); judicial intervention (max. 15 years); disqualification from contracting with the public sector; or a permanent prohibition from carrying out certain activities in whose exercise the offence was committed.	Loss of reputation due to events affecting the Group's image that may give rise to public campaigns against it, with repercussions, including at international level.

Likelihood of Occurrence: The probability that a risk will materialise into an actual event before taking into account the controls implemented to mitigate the inherent risk. The likelihood assessment considers the number of functions in which the risk may materialise and the company's historical background. It is assessed on a scale from 0 to 5.

PROBABILITY OF OCCURRENCE	
Very High (85% < P ≤ 100%)	5
High (65% < P ≤ 85%)	4
Medium (40% < P ≤ 65%)	3
Low (15% < P ≤ 40%)	2
Very Low (0% < P ≤ 15%)	1

Accordingly, the Criminal Risk Map displays risks ranging from the most significant (highest impact and likelihood) to the least significant, following the scheme below:

IMPACT						
Very low	Low	Medium	High	Very high		CRITICALITY INDEX (CI)
LIQUIDITY TENSION > 1 MONTH	WITHIN THE DIRECTORATE	COMPANY NEEDS FINANCING	CAPITAL REDUCTION / PROHIBITIONS	DISSOLUTION / COMPANY TERMINATION	CRIMINAL CONVICTION / ADMINISTRATIVE SANCTION	
DOES NOT REACH THE MARKET	APPEARS IN LOCAL MEDIA	REACHES STAKEHOLDER GROUPS / NATIONAL MEDIA	AFFECTS IMAGE / FRONT PAGES OF NATIONAL MEDIA	PUBLIC CAMPAIGNS AGAINST THE COMPANY AT NATIONAL AND INTERNATIONAL LEVEL	REPUTATIONAL DAMAGE	
5	10	15	20	25	Very high 85% < P ≤ 100%	PROBABILITY
4	8	12	16	20	High 65% < P ≤ 85%	
3	6	9	12	15	Medium 40% < P ≤ 65%	
2	4	6	8	10	Low 15% < P ≤ 40%	
1	2	3	4	5	Very low 0% < P ≤ 15%	
					1 to 6	
					8 to 12	
					15 to 20	
					25	
Threat						

RESIDUAL RISK:

Based on the preliminary analysis carried out, a corrective adjustment must then be performed through an assessment of the level of controls existing at Navantia to address each of the offences identified.

Residual risk is therefore the level of risk that remains within the company after the controls designed for its prevention or mitigation have been applied. The resulting residual risk level is determined through the assessment of the following criteria:

#	Types of Control Level	Classification		
1	Degree of automation	Automatic	These are controls of a mechanical nature. They are characterized by the fact that, once the control has been designed, its execution is not accompanied by subjective assessment or any human intervention.	3
		Semi-automatic	These are controls of a mechanical nature or which are performed mechanically and with a manual component.	2
		Manual	These are controls characterized by the fact that the execution of the control activity is normally accompanied by a greater or lesser degree of assessment.	1
2	Nature	Preventive	These are controls used to prevent errors or omissions that could occur in the Financial Statements.	3
		Detective	These are controls that identify and correct an error or omission that has occurred in the Financial Statements.	2
		Corrective	These are controls that ensure corrective actions are taken to avoid the recurrence of an event that has caused an error or omission in the Financial Statements.	1
3	Control sufficiency	Sufficient	Current controls are sufficient.	5
		Sufficient, with improvements	Controls exist, but with some recommendation.	4
		Medium	The control level is improvable.	3
		Medium Low	The control level is highly improvable.	2
		Insufficient	Controls do not exist or the risk is not mitigable.	1
4	Self-assessment	No incidents	No incidents exist.	5
		Minor incident	One or more minor incidents exist.	4
		Medium incident	One or more incidents of medium significance exist.	3
		Serious incident	One or more serious incidents exist.	2
		Very serious incident	One or more very serious incidents exist.	1
5	Internal Audit	Effective controls, no incidents	All controls are effective.	5
		Effective controls, with recommendation	All controls are effective, except for one control with an incident.	4
		Between one and five incidents	Effective controls, with between 1 and 5 controls showing an incident.	3
		Between five and ten incidents	Effective controls, with between 5 and 10 controls showing an incident.	2
		Ineffective Controls	Ineffective Controls.	1

Following this reassessment process, Navantia obtained the following results.

# Risk	Risk	Residual Impact	Residual Probability	Prioritisatior	Residual 2025	Residual 2024	Change
R.1 / R.2 / R.3 / R.4	Public Corruption / Illegal Financing of Political Parties	4,25	2,04	●	2,94	2,60	▲
R.5	Bribery in Business	3,38	2,25	●	2,76	2,66	▲
R.6	Fraud	2,25	1,50	●	1,84	1,84	◀▶
R.7	Misleading Advertising	2,63	1,20	●	1,77	1,77	◀▶
R.8	Breach of Trade Secrets	2,28	1,56	●	1,88	1,88	◀▶
R.9 / R.10	Subsidy Fraud / Fraudulent Obtaining of European Union Funds	2,25	1,20	●	1,64	1,64	◀▶
R.11	Tax Fraud	1,95	1,04	●	1,42	1,42	◀▶
R.12	Social Security Fraud	1,63	1,17	●	1,38	1,38	◀▶
R.13	Non-compliance with and Falsification of Accounting Obligations	1,38	0,88	●	1,10	1,30	▼
R.14	Offences Against Natural Resources and the Environment	2,93	1,43	●	2,05	2,05	◀▶
R.15 / R.16	Punishable Insolvency / Obstruction of Enforcement Proceedings	2,63	1,35	●	1,88	1,88	◀▶
R.17 / R.18	Offences Relating to Intellectual and Industrial Property	1,95	1,17	●	1,51	1,74	▼
R.19	Cybercrime	1,93	0,77	●	1,22	1,44	▼
R.20	Urban Planning Offences	2,63	1,05	●	1,66	1,66	◀▶
R.21	Offences Against Personal and Family Privacy	1,88	1,50	●	1,68	1,68	◀▶
R.22	Offences Relating to Ionising Radiation	3,00	1,50	●	2,12	1,84	▲
R.23	Offences Creating Risks Through Explosives	3,00	1,05	●	1,77	1,54	▲
R.24	Offences Against the Rights of Foreign Nationals	2,60	1,04	●	1,64	1,90	▼
R.25	Public Health Offences	1,95	1,17	●	1,51	1,51	◀▶
R.26	Smuggling	2,63	1,50	●	1,98	1,98	◀▶
R.27	Money Laundering and Terrorist Financing	2,60	1,43	●	1,93	1,93	◀▶
R.28	Misappropriation of Public Funds	2,60	1,56	●	2,01	2,01	◀▶
R.29	Bid Rigging and Manipulation of Prices in Public Tenders and Auctions	2,28	1,04	●	1,54	1,77	▼
R.30	Offences Against Workers' Rights	2,60	1,82	●	2,18	2,18	◀▶
R.31 / R.32	Offences Against Moral Integrity and Sexual Freedom	1,88	2,55	●	2,19	2,12	▲
R.33	Animal Welfare Offences	1,13	1,35	●	1,23	1,23	◀▶
R.34	Disclosure of Secrets Relating to National Defence	1,63	1,43	●	1,52	1,76	▼
R.35	UK Bribery Act 2010	4,25	2,04	●	2,94	2,6	▲
R.36	Facilitating UK and Foreign Tax Evasion	2,25	1,20	●	1,64	1,42	▲
R.37	FAILURE TO PREVENT FRAUD OFFENCE	3,83	2,38	●	3,02	2,66	▲