Entity-Specific

CYBERSECURITY AND DATA PROCESSING

SBM-3 - MATERIAL IMPACTS, RISKS, AND OPPORTUNITIES AND THEIR INTERACTION WITH STRATEGY AND BUSINESS MODEL

Entity-specific	Stage*	Description	Likelihood of occurrence	Time horizon
Cybersecurity				
(+) Impact	OP, Pt	Prevention and/or mitigation of incidents that could affect the integrity of the infrastructure managed by the Company, as well as the integrity and privacy of individuals, and/or the environment.	Current	S
(+) Impact	VC	Improvement of the cybersecurity culture among the Company's stakeholders.	Current	S
(-) Impact	VC	Occurrence of incidents that could impact on the integrity of the infrastructure managed by the Company, the integrity and privacy of individuals, and/or the environment.	Current	S
Risk	VC	Sophisticated cyberattacks that impact on the Company's operations, productivity, information, intellectual property, or image/reputation, as well as the integrity of individuals.		S
Risk	VC	Severe fines and penalties for breaches of regulations and enforcement control frameworks.		S
Opportunity	VC	Security as as a driver of business, reinforcing the company’s competitive edge through advanced security practices and high levels of compliance.		S
Opportunity	VC	Improvement of corporate governance and trust in the Company.		S

** OP: Own operations; VC: Value chain; Pu: Purchases; C: Customers; Pt: Partners; S: Short term; M: Medium term; L: Long term.*

MDR-P: POLICIES

Ferrovial has a Corporate Cybersecurity Policy in place approved by the CEO in 2022.The policy applies to all divisions and subsidiaries and can be consulted on the Company's website. Its principles and objectives are aligned with the business strategy. It is implemented by means of Security Policies that encompass organization, people, processes, and technologies, formalized in a set of Security Principles based on best industry practices, notably the NIST CSF and the ISO 27001 standard, under which Ferrovial has been certified since 2012).

Policy	Cybersecurity Policy
Description	This policy defines the principles and guidelines for safeguarding Ferrovial's information, systems, and operations against cyber threats, ensuring the confidentiality, integrity, and availability of digital assets. It supports the organization's commitment to business continuity and secure data management.
Objective	The policy aims to: • Ensure a digital and technological environment with the necessary level of security. • Guarantee legal, regulatory, and contractual compliance. • Ensure operational resilience against cyberattacks. • Foster a culture of awareness and responsibility in cybersecurity among employees, suppliers, and partners.
Associated material impacts, risks, and opportunities	• Material impacts: Potential financial losses, reputational damage, legal, regulatory, and contractual non-compliance, and disruptions due to cyber incidents. • Risks: Sophisticated cyberattacks that affect operations, productivity, information, intellectual property, or the Company's image/reputation, as well as the integrity of individuals. Severe fines and penalties for non-compliance with regulations and enforcement control frameworks. • Opportunities: Building stakeholder trust through robust cybersecurity practices, leveraging innovation for competitive advantage, and compliance with global regulatory standards to strengthen market positioning.
Follow-up and remediation process	Ferrovial ensures the implementation and compliance of the Cybersecurity Policy through regular reviews of risks and controls covering all business units and participated assets. This information is reported periodically to the Company's governing bodies that oversee the status of cybersecurity.
Scope of the policy	
Affected stakeholders	All Ferrovial employees, suppliers, and customers with access to Company systems or data.
Geographic areas	Global
Value chain application	The policy extends across the entire value chain, including suppliers and customers, ensuring secure practices in all business interactions. Cybersecurity is a practice that supports digital assets that ultimately support business activities.
Exclusions from the application	There are currently no exclusions; the policy applies to all areas of activity, geographies, and stakeholders globally.

Policy approval flow	
Responsible party	Chief Executive Officer (CEO) - responsible for approving and implementing the policy
Other issues to report (if applicable)	
Consistency with third-party instruments or standards	The policy complies with: • International standards, including ISO 27001 • European regulations such as the GDPR • The Spanish National Security Scheme (ENS) • Ferrovial's Corporate Responsibility and Sustainability Policies
Stakeholder engagement	The policy incorporates feedback from key stakeholders to effectively address cybersecurity issues and ensure secure collaboration across the organization.
How it is made available	This policy is available on Ferrovial's website (ferrovial.com) and on the intranet.
Significant policy changes	N/A - no changes have been made.

"Associated material impacts, risks, and opportunities" is a concept related to ESRS and double materiality. It is NOT related to the materiality of cyber incidents considered by the SEC.

MDR-A: ACTIONS

THE THREAT DETECTION, CORRELATION, AND CYBERINTELLIGENCE MODEL

The Company has SOC (*Security Operations Center*) capabilities to protect its data centers, perimeters, endpoints, and cloud environments. This service responds to alerts generated by SIEM (*Security Information and Event Management*) tools and detects events in accordance with use cases defined by Ferrovial's Cybersecurity Department.

There is currently a SOAR (*Security Orchestration Automation and Response*) platform that enables the coordinated integration and operation of various prevention and protection tools, facilitating automated detection and response, as well as the orchestration of activities for the containment, resolution, and neutralization of threats.

The organization integrates advanced cybersecurity capabilities for the protection against threats and the detection of information-related compromises, such as unauthorized access, anomalous transmission of large volumes of data, and exfiltration, whether through physical storage or cloud services.

Cyber intelligence capabilities expand threat detection processes and enhance response capabilities by identifying Indicators of Compromise (IoCs) and Tactics, Techniques, and Procedures (TTPs) used by cyber-offenders to carry out their attacks. Threat hunting exercises are also run to identify potential compromises that have not been previously detected.

Finally, the Company exchanges information on threats and manages incidents in coordination with national and international cybersecurity agencies when appropriate.

RESPONSE TO CYBERATTACKS

The Company has a CSIRT (*Computer Security Incident Response Team*) that responds to events detected by the SOC (Security Operations Center) that may become security incidents. This team has DFIR (*Digital Forensics and Incident Response*) capabilities to analyze, contain, mitigate, and prevent such events. The periodic identification of IoCs (*Indicators of Compromise*) and TTPs (*Tactics, Techniques, and Procedures*) are key to improving protection and detection mechanisms and the SOC's response, both manual and automated.

Likewise, Ferrovial has cybersecurity posture tools that enable real-time assessment of compliance with specific security parameters and controls, of the managed IT infrastructure (in data centers and cloud environments) and of *endpoints*. This provides a comprehensive overview of the risks and controls related to security recommendations issued by manufacturers, market standards, and security frameworks, as well as enabling the development of action plans to improve posture.

The capabilities and processes described above are driven by generative artificial intelligence, both for optimization purposes and to counteract new techniques applied by cyber-offenders who also rely on these technologies.

Ferrovial has an incident response protocol based on best market practices (INCIBE-CERT Guide, ISO/IEC 27035, and NIST). In addition, a global procedure has been implemented for the identification and reporting of material cyber incidents to regulatory bodies (SEC, national and international cybersecurity agencies, AEPD, among others). Communication with regulators, authorities, customers, and other stakeholders, through mechanisms within specific time frames, is one of the key elements for Ferrovial to ensure transparency and due diligence.

Detection and response capabilities are systematically evaluated through *Breach & Attack and Pentesting simulations*, using commercially available technologies (Cymulate and Pentera, respectively).

It is important to note that, during 2025, there were no material cybersecurity breaches in Ferrovial's information systems. Approximately 3.165 incidents were handled by the CSIRT and Ferrovial’s Cybersecurity team.

RESILIENCE AND CYBER-RESILIENCE

The Company established Contingency and Recovery Plans to respond to and recover from disruptive events, when required. Ferrovial is currently invested in the evolution of the Continuity model, with the aim of adopting a more global approach to standardize practices across all of the Company's business divisions.

These Contingency Plans cover crisis scenarios triggered by cyber threats. There is a Cyber Crisis Committee responsible for managing this type of incident. Likewise, Ferrovial has a procedure in place for reporting incidents to regulators and other stakeholders within this area.

Ferrovial, aware of the importance of resilience in its supply chain, incorporates the verification of contingency and recovery plans into the *Vendor Risk Management* (VRM) process, in the context of the service provided to the Company.

The business continuity model establishes the need to conduct regular testing of the plans, which is why Table-Top and Disaster Recovery Plan tests have been carried out throughout the year. The results have been positive overall, and opportunities for improvement have been identified, currently being implemented.

The Company maintains a cyber insurance policy, having expanded the limits and types of coverage for disruptive events and cyber incidents that may occur in the context of the activities carried out by Ferrovial, its business units, and subsidiaries; these include financial coverage, incident response, and legal advice. It should be noted that in 2025 it was not necessary to activate this policy, as no material cyber incidents have taken place.

THIRD-PARTY RISK MANAGEMENT

Ferrovial's Vendor Risk Management (VRM) program defines the security requirements third parties must meet, depending on the type of service they provide to the Company and the level of access they have to its information and digital assets.

In 2025, the supplier *onboarding* process has been automated and systematized, and the *monitoring* of suppliers that provide recurring services to Ferrovial is currently undergoing automation and systematization processes.

The VRM process assesses the accreditations, certifications, qualifications, and evidence that attest to the level of security compliance of the relevant product or service provided by the vendor, as well as the level of security maturity the vendor can prove. If material risks are identified during the review processes, appropriate measures are taken, including contract termination.

Third-party risk management ensures that cyber incidents that may affect Ferrovial are reported in a timely manner, and that response and recovery plans are in place should they be necessary.

EXTERNAL VERIFICATION AND VULNERABILITY ANALYSIS

As part of Ferrovial's continuous improvement process, it is essential to carry out both internal and external audits to identify vulnerabilities and areas for improvement, the implementation of which will strengthen cybersecurity and contribute to the mitigation of risks.

The following are the reviews and audits being carried out on a recurring basis within the organization:

- Internal and third-party audits based on the ISO 27001 certification.
- Integrated SOX audits:
  - ITGC controls.
  - Cybersecurity model controls.
- External audit by SWIFT (*Society for Worldwide Interbank Financial Telecommunication*).
- Audits carried out by Internal Audit (third line of defense) in accordance with their annual plan (two or three annual audits).
- Questionnaires, security approvals required by Ferrovial's clients.
- Dow Jones Best-in-Class Index.
- ESG Sustainability Report (double materiality).
- Ad hoc security reviews according to annual planning.
- *Breach & attack*, and recurring pentesting based on Cymulate and Pentera tools, according to annual planning.
- Threat Hunting & Compromise Assessment reviews to identify potential compromises/breaches not detected by monitoring systems
- Vulnerability review in data centers, endpoints, perimeters, and cloud environments, as well as in industrial environments.
- Review of vulnerabilities in source code.
- Review of Ferrovial's cybersecurity rating through *BitSight*.
- Vendor security risk reviews (*Vendor Risk Management*).
- Crisis simulations (*tabletop exercises*).
- Posture management provided by cybersecurity tools (*Microsoft Compliance and Wiz*).

The Cybersecurity Department consolidates, assigns, plans, and supervises the implementation of the different action plans arising from the assessments, reviews, and audits carried out.

The management review process is formally conducted on a yearly basis, one of its purposes being the review of the achievement level corresponding to planned cybersecurity actions. This process is supervised by the Global CISO, taking into account a number of data, such as KGIs and KPIs, the results of audit and review processes, and the monitoring of risk treatment plans.

MDR-T: TARGETS

The objectives defined in the Corporate Cybersecurity Policy are measured using Key Goal Indicators (KGIs) defined in the Information Security Management System (ISMS), which is based on the ISO 27001 standard, audited on an annual basis by BSI. This allows for monitoring the effectiveness of the Policy's implementation. The indicators are based on measurements of organizational, technological, and process capabilities related to cybersecurity, associated with each of the Strategic Objectives established in the Policy.

Some of the main targets are aimed at:

- Ensuring a digital and technological environment with the necessary level of security.
- Guaranteeing legal, regulatory, and contractual compliance.
- Properly managing security incidents and building resilience to them.
- Promoting an appropriate security culture.
- Harmonizing security across different business units and subsidiaries.
- Facilitating digitization, innovation, and the adoption of new technologies to support the business.
- Facilitating business opportunities and bidding processes.
- Establishing strategic partnerships in the area of security.
- Fostering a culture of awareness and responsibility in cybersecurity among employees, suppliers, and partners.

MDR-M: METRICS

100% of security incidents successfully managed	193,592 phishing simulation emails received by employees annually	11,431 unique users included in phishing simulations annually
61,538 phishing emails blocked per month by the company's systems	14,991 attempts to access corporate resources blocked (malicious/untrustworthy source) per month	9.3 ransomware attacks detected and automatically blocked per month

Security incidents

In 2025, 100% of security incidents were successfully managed. The objective of this indicator is to verify that the security incidents occurring at Ferrovial are managed in the best possible way to mitigate their potential impact. Only those incidents managed by the Cybersecurity Department are included in this review, covering all business divisions using Corporate Digital Products and Services. The measurement criterion is the ratio of incidents properly managed versus the total number of incidents registered in the reference period, based on response time, actions taken, follow-up and evidence gathering, resolution, root cause analysis proportionate to the incident type and lessons learned. The provided data corresponds to the annual average, calculated from all monthly measurements collected during the year from January 2025 to December 2025. This control forms part of the SOX Cybersecurity framework, and is reviewed by the external auditor PwC.

Phishing simulation emails received by employees

In 2025, employees received a total of 193,592 phishing simulation emails, as part of regular and systematic training aimed at strengthening users' ability to identify potential threats. This metric is based on the number of emails issued through the awareness platform during simulated phishing campaigns, limited to users managed by the Corporate Cybersecurity Department, covering from January to December 2025. The KPI is integrated into the Information Security Management System (ISMS) and is audited externally by BSI under ISO 27001 certification, ensuring the robustness and traceability of the process.

Users included in phishing simulations

Throughout 2025, 11,431 unique users participated in phishing simulations. The indicator reflects the number of unique users registered on the awareness platform and involved in phishing simulations. It applies exclusively to users managed by the Corporate Cybersecurity Department and uses the number of unique users registered on the KnowBe4 platform. This KPI forms part in the ISMS, and undergoes external audit (BSI) required for ISO 27001 certification.

Blocked phishing emails

The company's systems blocked an average of 61,538 phishing emails per month, across 2025, demonstrating the effectiveness and quality of the filtering capabilities of the MS Defender platform. The metric is calculated based on the total number of phishing, malware, impersonation-blocked emails and policy-blocked messages, excluding spam. It applies only to users under the Corporate Cybersecurity Department, and reflects an annual average of monthly measurements collected between January and December 2025. The KPI is incorporated into the Information Security Management System (ISMS) and is subject to external audit by BSI under ISO 27001 certification, ensuring rigorous oversight and verification.

Blocked attempts to access corporate resources

In 2025, the company blocked an average of 14,991 attempts per month to access corporate resources from malicious or untrustworthy sources, demonstrating the effectiveness and quality of the communications filtering performed by the MS Defender platform. This indicator is based on the number of malicious domains, IPs and URLs blocked, and covers users managed by the Corporate Cybersecurity Department, following the annual average calculated from all monthly measurements collected between January and December 2025. The KPI forms part of the Information Security Management System (ISMS) and is audited externally by BSI under ISO 27001 certification, ensuring rigorous oversight and verification.

Ransomware attacks detected and automatically blocked

In 2025, an annual average of 9.3 ransomware attacks were detected and automatically blocked per month. This indicator measures the effectiveness of detection and protection capabilities against ransomware, after the (manual) exclusion of potential false positive and covers only users managed by the Corporate Cybersecurity Department, using the measurement criterion of Microsoft Defender (XDR), after manually filtering potential false positives. This KPI is included in the ISMS, and subject to external audit (BSI) required for ISO 27001 certification.

INNOVATION, DIGITALIZATION AND TECHNOLOGY APPLIED TO BUSINESS

SBM-3 - MATERIAL IMPACTS, RISKS AND OPPORTUNITIES AND THEIR INTERACTION WITH STRATEGY AND BUSINESS MODEL

The rapid evolution of digital technologies generates material impacts that transform Ferrovial's business model, creating both risks and strategic opportunities. Cross-cutting digitalization and the accelerated adoption of emerging technologies improve efficiency, competitiveness and operational resilience, but also increase exposure to cyber threats, privacy risks, technological obsolescence and regulatory pressure. These factors require ongoing investment in digital capabilities and strong governance to ensure the sustainability of changes.

The ReadIT 2027 strategy is implemented as a response to this environment by integrating innovation, resilience and value creation within a framework directly applied to business targets. The most relevant impacts include the transformation of processes and platforms, migration to the cloud and the adoption of artificial intelligence, reducing timelines, optimizing costs and enabling new data-based business models. However, these advances come with critical risks: cybersecurity vulnerabilities that can compromise assets and reputation, potential regulatory non-compliance in increasingly demanding environments, and cultural reluctance that limits adoption and reduces returns on investment (ROI).

In the face of these risks, material opportunities emerge, strengthening Ferrovial's competitive position: the automation of tasks and workflows, the creation of scalable digital products, collaboration with startups in the fields of robotics, digital twins and virtual reality, as well as the exploitation of advanced analytics for data-driven decisions. The interaction between these elements is structured through initiatives ensuring operational resilience –such as the improvement of cybersecurity posture, obsolescence monitoring and the automation of SOX controls– while promoting open innovation and technological experimentation in real use cases.

Additionally, the investment in artificial intelligence initiatives and the associated governance framework reflects Ferrovial's commitment to a sustainable and structured integration of AI into processes and platforms, reducing risks associated with accelerated adoption and ensuring positive long-term impacts. This strategy not only mitigates threats but also turns digital transformation into a driver of efficiency, competitiveness and diversification, aligning each initiative with the corporate objectives and targets defined for 2027.

Ferrovial assumes that technological innovation must come with responsibility, transparency and alignment with corporate values. For this reason, it has defined a governance and ethical principles framework that guides the development and application of AI solutions in all business areas. This framework is built around five core pillars:

1. **Transparency and explainability**

   Each model must be understandable and auditable, ensuring that automated decisions can be explained to internal teams and stakeholders. This aspect reinforces trust and accountability.

2. **Human supervision in critical decisions**

   The "human in the loop" principle is applied to ensure that AI acts as a support tool, not a substitute for professional judgment, especially in sensitive processes.

3. **Data protection and privacy**

   All solutions comply with the GDPR and applicable regulations, incorporating anonymization and encryption techniques to safeguard customer, employee and partner information.

4. **Equity and Bias Mitigation**

   Continuous validation processes are established to detect and correct biases in data and algorithms, avoiding discriminatory impacts and ensuring fair results.

5. **Sustainability and ESG alignment**

   AI is assessed not only for its economic impact, but also for its contribution to sustainability and social responsibility targets, in line with Ferrovial's ESG commitments.

To facilitate safe adoption, the Company has developed internal manuals and training programs that include practical recommendations for the use of tools such as Microsoft Copilot and other generative solutions. These resources are available on the AI portal in MyForum, which centralizes documents, use cases, and communities of practice to drive a culture of digital accountability.

Ferrovial also set up review committees and ethical impact metrics that oversee the consistency between technological innovation and corporate values. This approach is complemented by the observation of international regulatory frameworks, such as the European AI Regulation, to anticipate requirements and ensure regulatory compliance.

In short, AI is not only conceived as an engine of efficiency and competitiveness, but also as a catalyst for trust, sustainability and social value, ensuring that each technological advance reinforces corporate reputation and purpose.

Entity-specific	Stage*	Description	Likelihood of occurrence	Time horizon
Innovation, digitalization and technologies applied to the activity				
(+) Impact	OP, Pt	Promotion of an innovative and digital culture that fosters the Group's continuous improvement and generates a friendlier work environment.	Current	S
(+) Impact	OP, Pt	Promotion of innovation and digitalization to improve safety in projects, reducing accidents and risks for workers.	Current	S
(+) Impact	OP, Pt	Generation of innovation in society through the creation of research centers by means of the development of collaborations and alliances.	Current	S
(+) Impact	OP, Pt	Improvement in the environmental impact of of the company's projects (energy efficiency, emission reduction, etc.) as a result of the implementation of new technologies in the product process and digital management tools that help quantify their impact.	Current	S
(-) Impact	OP, Pt	Issues related to the maintenance and replacement of machinery adapted to new technologies.	Current	S
(-) Impact	OP	Impact on employee roles and career progression in the context of evolving digital transformation competencies and requirements.	Current	S
(-) Impact	OP	Workforce displacement and role transformation resulting from automation and adoption of new technologies.	Current	S
Risk	OP, Pt	Vulnerability in operations due to service discontinuations resulting from exposure to natural disasters.		S
Risk	OP, Pt	Potential fines and loss of reputation due to regulatory non-compliance in AI matters.		M
Opportunity	OP, Pt	Implementation of new technologies that generate a more resilient asset portfolio.		M
Opportunity	OP, Pt	Identification of new businesses based on the evaluation of new low-emission technologies (photovoltaic plants, nuclear SMRs, offshore wind energy, etc.).		M

** OP: Own operations; VC: Value Chain; Pu: Purchases; C: Customers; Pt: Partners; S: Short term; M: Medium term; L: Long term.*

MDR-P: POLICIES

Ferrovial manages innovation programs and initiatives through a structured, cross-cutting policy aligned with the Company's vision of the future. This policy, led by senior management, extends across all areas and employees at Ferrovial, and is implemented by a specialized team that manages key areas such as open innovation, growth, asset management, sustainability and the development of new business models. Each of these areas is organized into cross-cutting programs and overseen by project managers.

Ferrovial's Innovation Policy positions innovation as a core driver for anticipating and leading the transformation of the sector, while generating sustainable and differentiated value for both the Company and society as a whole. The policy is grounded in principles such as a transformative mindset, integration of digital capabilities and advanced technologies, open collaboration with internal and external players, operational excellence, and a strong focus on sustainability and social commitment. It also ensures that innovation practices evolve in alignment with emerging regulatory frameworks such as the EU AI Act, incorporating responsible design principles and internal guidance to support the ethical, safe and compliant development of advanced technologies.

The Innovation Policy is currently cross-functional and applies across all of Ferrovial's business lines. Ferrovial has formalized a global Innovation Policy that reflects all the efforts already underway in the field of innovation, and which is periodically reviewed to ensure alignment with environmental challenges and trends in the sector.

The **Innovation Policy** is designed to:

- Promote the identification and development of innovation opportunities in all areas of Ferrovial, anticipating trends and challenges within the sector.
- Deploy new products, operations, and technologies that increase productivity, strengthen resilience, and generate sustainable competitive advantages.
- Promote innovation models that integrate sustainability, social responsibility and economic viability criteria, ensuring a positive impact on the environment.
- Promote a culture of innovation grounded in the principles of collaboration, continuous learning and recognition, empowering talent and adapting to change.
- Rigorously evaluate the impact of initiatives, ensuring their tangible contribution to strategic targets and the value generated for business units.

Ferrovial's innovation ecosystem is open and collaborative, based on co-creation and the pursuit of synergies across the global ecosystem. Priority is given to the continuous improvement of processes and integration of platforms, ensuring alignment with corporate standards and optimization of resources.

Ferrovial fosters the development of digital skills and the use of advanced tools, promoting a culture of continuous learning and adaptability to change. Innovation is focused on generating a positive impact on society and the environment, integrating sustainability, safety, ethics and compliance criteria across all initiatives.

The Innovation Policy is rigorously and regularly evaluated, reflecting Ferrovial's commitment to anticipating trends, diversifying and adapting the business model sustainably.

MDR-A: ACTIONS

Ferrovial is undergoing a significant digital transformation aimed at enhancing its competitiveness and evolving its businesses and operations. The Company seeks to position itself as a benchmark in the use of data, technology and innovation, and to this end has defined its mission and targets through the ReadIT 2027 program, which serves as the strategic framework for digitalization and technological modernization.

The ReadIT 2027 strategy is structured around four core pillars that guide all transformation initiatives:

- **Innovation Levers:** This pillar fosters the generation and adoption of new technologies, encourages open collaboration with external agents and promotes the development of innovative business models. The goal is to experiment with advanced solutions, activate growth opportunities, and consolidate asset management in an efficient and sustainable manner.
- **Areas of focus:** This pillar brings together initiatives related to intelligent data management, automation and digitalization of processes, integration of technological platforms, development of digital skills in people and the creation of digital products and solutions based on artificial intelligence. The aim is to optimize decision-making, streamline workflows and enhance the organization's ability to adapt.
- **Fundamentals:** This pillar guarantees sustainability and social commitment, reinforces operational resilience and ensures regulatory compliance. It includes responsible management of environmental, social and governance (ESG) aspects, protection against technological risks and continuous monitoring of obsolescence, ensuring a robust and future-ready business model.
- **Value Levers:** This pillar focuses on maximizing efficiency, strengthening risk management, improving competitiveness and facilitating the transformation and diversification of the Company. The value generated translates into tangible results for the different business units, aligning the digital strategy with corporate objectives.

Each of these pillars incorporates specific variables and key performance indicators (KPIs) with specific targets for 2027, enabling the monitoring of progress and the tangible impact of digital transformation in areas such as the adoption of data platforms, process automation, digital training, efficient asset management, sustainability and operational resilience.

The ReadIT 2027 program is designed to strengthen Ferrovial's core business, focusing on automation, efficiency, competitiveness, agility and data monetization, while fostering a digital business culture.

To ensure the effectiveness of these initiatives, Ferrovial implemented monitoring and control mechanisms that allow the progress and impact of the strategy to be evaluated. These mechanisms include:

- **The use of key performance indicators (KPIs)** to track the degree of progress in each of the strategic pillars and to ensure compliance with the targets defined for 2027.
- **Data management and protection and cybersecurity,** supported by regulatory frameworks and specialized tools that ensure operational resilience and compliance with regulatory standards.
- **Technology governance,** underpinned by standardized models that facilitate the integration and oversight of digital platforms and systems throughout the organization.
- **Training and digital skills development,** through dedicated programs and learning pathways that promote the adoption of new technologies and the use of advanced tools such as AI and automation.
- **Sustainability impact (ESG) monitoring,** ensuring that digital initiatives make a tangible contribution to environmental, social and governance targets, and that these are monitored in an automated and transparent manner.

The strategy establishes quantifiable, time-bound targets linked to sustainability and operational excellence, including increased digitalization and automation, the deployment of scalable AI solutions, enhanced cybersecurity resilience, and the strengthening of the ESG strategy. These targets are monitored by KPIs aligned with the four strategic pillars and are continuously evaluated through regular reporting, AI-based process optimizations, risk tracking, and evolution of sustainability initiatives.

Stakeholder engagement plays a critical role, encompassing collaboration across business units, partnerships with technology providers, engagement with regulatory bodies, and information loops with employees and industry experts. Future developments include ongoing performance monitoring, refinement of sustainability-focused initiatives, and greater stakeholder engagement to ensure alignment with evolving ESG and digital transformation expectations.

This structured approach ensures that ReadIT 2027 aligns with Ferrovial's broader corporate sustainability and business resilience targets while remaining adaptable to new challenges and opportunities. The program is built around value levers, from which the necessary capabilities are extracted to digitize the business and the Company as a whole.

During 2025, Ferrovial advanced the ReadIT 2027 strategy through a focused set of research and development initiatives aimed at strengthening the Company’s digital foundations and accelerating the transformation of its infrastructure and mobility businesses. These efforts continued to evolve across three strategic pillars—Innovation Levers, Focus Areas, and Fundamentals—each contributing to a more efficient, data-driven and resilient operating model.

Under the Innovation Levers pillar, Ferrovial expanded its capacity to validate emerging technologies in realistic operational environments. The Company strengthened the capabilities of Ferrovial Lab, where multi-sensor edge architectures, real-time data-fusion engines, and cloud-to-edge connectivity models were tested to support next-generation Intelligent Transportation Systems (ITS) and automation use cases. This environment also enabled the integration of digital-twin representations, providing real-time visualization of detections and operational events. In parallel, Ferrovial advanced autonomous-construction technologies, where GPS-guided machine-control systems improved execution precision, enhanced safety conditions, and generated automated quality-assurance/quality-control (QA/QC) datasets. The Company also progressed its long-standing research collaboration with the Massachusetts Institute of Technology (MIT), particularly in predictive geotechnical modelling and advanced soil-monitoring technologies, reinforcing Ferrovial’s capabilities in climate-resilient infrastructure design.

Within the Focus Areas pillar, Ferrovial continued building an integrated digital ecosystem that supports automation, analytical rigor and operational consistency. The Company made progress in the expansion of global platforms for transactional processes and the industrialization of cloud-based computer-vision systems, which enhanced automated incident detection, operational monitoring and safety analytics across several business units. Data-driven engineering also advanced through the evolution of the Smart Tunnels environment, which consolidated geotechnical models, machine telemetry, and historical production records into a unified analytical layer supporting more effective execution control and more accurate bidding processes. Ferrovial further strengthened its data-governance frameworks, including the mapping of end-to-end financial and operational data flows in its concessions business, improving the reliability, consistency and auditability of Traffic & Revenue (T&R) reporting.

The Fundamentals pillar focused on cybersecurity, regulatory compliance and sustainability-aligned innovation. In 2025, the Company enhanced its cybersecurity governance model to align with evolving international regulations, including the European Union NIS2 Directive (Network and Information Security Directive), U.S. Securities and Exchange Commission (SEC) rules on cyber governance and disclosure, and North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards. These updates strengthened business continuity capabilities, reinforced third-party risk management, and improved integration with the corporate Governance, Risk and Compliance (GRC) platform. Ferrovial also advanced data-protection efforts through comprehensive reviews of cross-border data flows, sensitive-data inventories, and alignment with applicable U.S. privacy requirements and international data-transfer frameworks. Sustainability-oriented innovation progressed through the development of carbon-capture research, particularly in membrane-based solutions applicable to industrial environments, and through the sensorization of asphalt plants to support efficiency improvements and emissions-reduction objectives.

Across all pillars, Ferrovial continued to apply standardized technology-governance models, cybersecurity and data-management frameworks, and Key Transformation Indicators (KTIs) that monitor technology adoption and the impact of digital initiatives. Together, the Company's 2025 R&D activities strengthened its technological foundations, enhanced operational resilience, and supported the development of innovative digital capabilities aligned with Ferrovial's long-term competitiveness and sustainability commitments.

Investment in innovation in 2025	
Total investment (€)	77,625,328.99
% of investment directly towards ESG projects	33.70

Note: See note 3.2 of the Consolidated Annual Accounts for further information.

MDR-T: TARGETS

Ferrovial has defined a comprehensive approach to target management and performance measurement within the framework of the ReadIT27 program, aligning strategy with operational execution and impact monitoring.

1. **Strategic KTIs and 2027 targets**

Ferrovial's strategy is structured around four core blocks or pillars, each supported by defined variables and technical indicators with specific targets for 2027. These blocks represent the strategic axes underpinning digital transformation and enable progress and performance to be monitored in key areas:

- **Innovation levers**: They drive transformation and growth by fostering the exploration of new technologies and business models, while ensuring that innovation is transversal and relevant across all areas of the Company.
- **Areas of focus:** They reinforce digitalization and operational excellence, promoting the efficient use of data, process automation, platform integration and the development of digital capabilities in the organization.
- **Fundamentals:** They guarantee sustainability, resilience and regulatory compliance, integrating ESG criteria, cybersecurity and technological surveillance to protect and strengthen the business model.
- **Value levers:** They translate value creation into efficiency, risk management, competitiveness and the ability to transform and diversify, aligning the results with Ferrovial's strategic targets.

2. **Impact model for initiative programs**

In addition to the strategic KTIs, each program and initiative has its own impact model, that defines individual and specific targets, enabling the ongoing measurement and evaluation of progress and value creation. This model includes:

- Definition of operational and impact KPIs at the program, workflow and initiative level, adapted to the nature and scope of each project.
- Regular monitoring of results, enabling data-driven decision-making and identifying areas for improvement.
- Continuous assessment of the impact on efficiency, resilience, sustainability, innovation and competitiveness, ensuring traceability and alignment with corporate targets.
- Transparent communication of progress and results to key stakeholders, reinforcing the culture of measurement and continuous improvement.

Through this approach, Ferrovial guarantees that both the strategic target and the specific targets corresponding to each program are clearly defined, measured and aligned with the transformation vision and the 2027 targets, ensuring the value creation and tangible impact in all areas of the Company.

Confidentiality and disclosure limitations

Certain detailed quantitative information regarding specific target levels, baseline values, intermediate milestones and methodologies has not been disclosed due to confidentiality and competitive sensitivity considerations, as such information forms part of Ferrovial's internal strategic planning and execution processes.

Nevertheless, Ferrovial confirms that all targets defined under the ReadIT27 framework are measurable, outcome-oriented and time-bound, are subject to regular monitoring through defined KPIs and governance mechanisms, and are aligned with the Company's strategic objectives and 2027 transformation roadmap.