Additional ESG information

Index

Supplementary information relating to the human resources area

Working conditions management programmes

In all business sectors in which it operates, A2A participates in the negotiation tables for national collective labour agreements (CCNLs, which constitute the sole reference collective bargaining framework for each sector), contributing to the definition of first-level employment conditions, periodically updated in line with inflation values recorded ex post and forecast for the coming years. The Group's remuneration principles have also been subject to analysis and validation by external certification bodies.
Within Group collective bargaining, overtime work is identified as a residual and exceptional instrument, subject to quantitative limits set by the CCNL and by company-level bargaining.
Remuneration policies are applied without any regard to the gender of the worker, with the Group adopting measures for the involvement of employee representatives in systems for monitoring any salary gaps, in full compliance with regulatory provisions.
Annual leave consists of periods of paid absence and, within Group bargaining, agreements are in place to foster the use of leave entitlements granted to each worker (annual leave – above the minimum established by law – permits and other forms of time "paid" by the company).
Collective dismissals are managed with notice periods extended compared with those established by Law 223/91, in order to manage, within the necessary timeframe, the co-construction of any accompanying pathways, primarily addressed to personnel closest to retirement.
Systems exist to verify compliance with working hours by the corporate population, a matter on which dialogue with employee representatives is ongoing, also with a view to identifying the best flexibility solutions.
Social protection extends beyond national provisions, providing healthcare, insurance and additional subsidies compared with those required by law.
Dialogue is also ongoing regarding the training needs of the company workforce, also with a view to the constant adaptation of skills to the evolution of working methods and technologies.

Employee support

A2A Life Caring is a plan supporting employee parenthood, a broad, comprehensive and cross-cutting programme that demonstrates the Group's concrete commitment to supporting birth rates in a historical phase characterised by the country's continuous demographic decline.
The main contents of the initiative are:

- Time/Maternity and paternity leave: in addition to the provisions of the law, employees may take one additional month of leave paid at 100% or, alternatively, opt for the payment through payroll of an equivalent one-off amount;
- Economic support: provision of contributions to support education and work-life balance, with the possibility of obtaining reimbursement for expenses incurred for education and schooling services (such as books, school fees and nursery schools), differentiated by age bracket, for each child up to 18 years of age;
- Culture: awareness-raising pathways for new parents with children aged 0 to 3 years and for their managers. These pathways support and accompany new parents in discovering and strengthening their abilities, helping them to put these abilities into practice in both private and working life. Managers also participate in this initiative with the aim of reinforcing positive managerial cultural models and offering useful suggestions to increasingly welcome and enhance the needs of their "new parent" employees;
- Culture: dissemination and awareness-raising activities through webinars dedicated to parenthood, as well as internal dissemination activities on fertility and procreation, including Medically Assisted Procreation.

The following are also available:

- the nursery school network of the "Cresciamo il Futuro" project (in collaboration with the Ministry of Labour and Social Policies, the initiative involves eight large Italian companies and provides a network of corporate and private nursery schools accessible to all people working for the participating companies);
- the Crescere Assieme nursery school and preschool located at the A2A premises in Brescia.

The Group also provides various support channels for caregivers: from information and training meetings to the possibility of requesting personalised case management, with assistance up to the activation of the services required for the care of one's loved one. Finally, there is the possibility of accessing a Portal that allows consultation of all opportunities made available by Public Welfare.

Approach to reorganisation processes

In parallel with listening to and supporting people, A2A also adopts a responsible approach in managing reorganisation processes, ensuring attention to the social sustainability of its choices and promoting dialogue with social partners. In 2024, some Group companies agreed with trade union organisations to activate collective dismissal procedures (intended to affect 2025 and also part of the current 2026), aimed at facilitating reorganisation and generational renewal processes through economic incentive mechanisms benefiting people close to pension eligibility.
With regard to business transfer procedures, each extraordinary transaction of the Group is accompanied by trade union consultation processes, useful for the joint identification (between the company and trade union organisations) of the best solutions to safeguard employment and ensure continuity of employment conditions.

Remote working and flexible working

A2A adopts a smart working model characterised by a high degree of flexibility and adaptability, built taking into account roles, activities and individual needs; the result is a tool that balances remote and in-person work, taking account of operational and team needs, with the objective of fostering collaboration, productivity and well-being. It is a model that allows remote working for between 20% and 60% of working time on a monthly or two-monthly basis, including half days, considering the role and activities.
Equally advanced is the range of flexibility tools (daily, intra-day, "trust-based" working hours) that allow a significant portion of the corporate perimeter to overcome the difficulties of the classic "rigid working hours" model.
Collective bargaining also offers time-bank instruments for accruing additional work and using it according to the worker's needs, as well as solutions for organising the weekly working schedule according to the so-called short Friday model.
Part-time work is a tool applied across all Business Units, with a degree of extension consistent with the type of activity and work organisation.

Mental health

One of the long-standing services made available by the Group to its people is Psychological Counselling: a space to take care of oneself and one's well-being, a support to face moments of difficulty or change, to gain awareness of experiences and emotions and to strengthen resources and strengths at every stage of one's life. Sessions may take place in person at the Group's main offices or remotely, without any limitation on the number of sessions that may be used.

Development and performance evaluation system

In A2A Group companies (including Acinque), there is a specific Performance Management process involving the entire population of executives, middle managers and white-collar employees, for a total of approximately 7,500 people. This process provides, on an annual basis, for an overall assessment of individual contribution and an assessment of behaviours demonstrated against the key competencies of the behavioural competency model. In the first phase of the process, the definition of one's individual contribution is envisaged through the description of one's activities, shared between the person and the manager, which may be updated. In the subsequent evaluation phase, each person is required to complete a self-assessment step, aimed at stimulating awareness and dialogue with managers, as well as the possibility of involving one or more "additional evaluators", in addition to direct managers, in order to collect multiple points of view and enrich feedback in the manager-person relationship. From 2026, the Performance Management process will also be extended to a pilot perimeter of personnel with worker qualification within the Smart Infrastructures BU, Generation and Trading BU and AEB (Reti più and Public Lighting) companies, for a total of approximately 850 people.
The annual performance management process described above is also supported (for A2A Group companies, excluding Acinque) by the presence of the "Anytime Feedback" session in the Smart People application, which allows feedback to be exchanged between managers and employees, and among colleagues. The objective is to foster a feedback culture within the Group and facilitate dialogue between people with a view to continuous improvement.
Also for A2A Group companies (excluding Acinque), an MBO bonus pool process is envisaged for executives and an MBO bonus pool process for a perimeter of non-executive personnel.

The MBO process provides for two types of objectives: Central objectives and Individual objectives identified by the Manager, also upon proposal by the MBO assignee.
The calculation mechanism of the incentive system provides for the incremental or decremental impact of the Group's economic-financial corrective factor, A2A as at 31 December of the relevant year, on the result bracket determined on the basis of the assessment of achievement of assigned objectives, carried out through optional self-reporting by the MBO assignee, approval by their Manager and validation by the BU / staff Unit MBO Representative.
The competency assessment affects the MBO payout only by halving it in the event of an inadequate result within the Performance Management process described above.
By contrast, the Acinque MBO system, which applies to the entire executive population and to certain middle-manager figures with a more direct impact on business results, provides for a variable component correlated to short-term performance, both with reference to individual performance and demonstrated competencies and to the results of the Company and the Group, taking into account the objectives defined in the strategic plan. The variable component provides for a maximum limit, with predetermined and measurable performance objectives linked to value creation for shareholders over an annual horizon. The process includes an initial objective-setting phase by March, a mid-year review phase and a final reporting phase at the beginning of the following year. The assessment of individual objectives is the responsibility of the Manager, supported by appropriate certification, while reporting of financial objectives is the responsibility of AFC and HR.

Methods for assessing and managing health and safety risks

The A2A Group manages health and safety risks through an integrated process combining the Risk Assessment Document (DVR), improvement plans, health surveillance and incident event management, with traceability through ARIAL.
OHS risk assessment is carried out in accordance with Legislative Decree 81/2008 and is formalised in the DVR, prepared with the involvement of line management and the designated figures (RSPP, Occupational Physician, RLS, managers and supervisors). In ARIAL, the assessment is organised by tasks/homogeneous groups (GOP/GOS) and exposure scenarios, with definition of severity and probability, prevention and protection measures and residual risk; the outcomes feed into protocols and health surveillance. Priorities are defined according to residual risk and translated into Action Plans tracked in ARIAL (objectives, responsibilities, resources and timelines), including ongoing monitoring of cases requiring attention. Emergency preparedness and response are integrated into the system: in the event of an incident, immediate protection and containment actions are activated and, where necessary, Emergency Plans and crisis management safeguards are activated, with the required communications and involvement of the competent HSEQ structures.
Progress is verified through monitoring of the advancement and effectiveness of actions (also through audit/monitoring outcomes and management of any non-conformities) and through periodic reporting on trends and indicators (e.g. injury rates, reports/near misses and action closure status). Inspections and site visits support hazard identification and DVR updating; the Occupational Physician carries out workplace inspections at least annually (unless otherwise indicated in the DVR), with minutes and follow-up actions. Investigation of incident events follows a structured flow (reporting, immediate actions, recording/classification, analysis and improvement actions): injury events are recorded in ARIAL within 48 hours (within 24 hours for injuries to Group workers), with management of reporting obligations to INAIL depending on prognosis; classification considers actual and potential consequences and the analysis generates actions monitored in ARIAL until effectiveness is verified and the DVR is updated where necessary.

Health and Safety management and awareness-raising for contractors
A2A oversees contractor health and safety through a pathway that accompanies the company from entry into the Supplier Register through to completion of on-site activities. The approach combines HSE pre-qualification, verification of requirements before start-up, operational induction and constant performance monitoring, in order to prevent injuries and promote safe behaviours throughout the supply chain.

Occupational health and safety training for contractors

HSE competence is a prerequisite: already during A2A qualification, evidence, questionnaires and, where applicable, certifications are collected, in order to verify that the company has adequate organisation and competencies. Before operational start-up, training is completed by site-specific information and training, consistent with the risks and measures defined in the safety documents (e.g. DUVRI/PSC/DIC).

Health and safety pre-qualification criteria for contractors
Selection favours qualified suppliers, assessed also for solidity, reputation and sustainability, including HSE aspects. Depending on the criticality of activities, qualification may be more streamlined or more in-depth, with

additional checks on requirements and documentation. Where appropriate, the pathway is completed by audits or field checks, useful to confirm the effective application of the required standards.

Health and safety induction on construction sites for contractors
Before accessing the site, the contractor is informed of operating rules, specific risks and methods of cooperation and coordination with the client. Start-up is supported by the relevant safety documentation (e.g. DUVRI/PSC/DIC) and by the checks necessary to finalise the order; for works and services subject to Article 26 and/or Title IV of Legislative Decree 81/08, a compliance check is also required, with any request for additions.

Continuous health and safety assessment processes for on-site contractors
During execution, A2A monitors contractors' HSE performance through risk and performance assessment tools, in order to promptly identify any signs of criticality. If deviations or non-conformities emerge, investigations, corrective actions and – where necessary – field checks are activated; in the most serious cases, consequent management measures are applied, in line with Group rules.

Overall, these safeguards strengthen the Group's Responsible Procurement approach and foster the dissemination of a prevention culture also among contractor companies.

Supplementary information relating to the business area

Asset Management System

With reference to the Smart Infrastructures Business Unit and the companies Unareti and Duereti, A2A adopts a structured approach to Asset Management throughout the entire asset life cycle.

The BU Asset Owner defines and updates the Asset Management Policy, which translates the mission and pillars of A2A's Industrial Plan into operational Asset Management objectives, clarifying management principles, priorities and decision-making criteria.

The Policy forms an integral part of the Strategic Asset Management Plan (SAMP), prepared by the Asset Manager, which details the asset management framework, planning and control processes and managerial responsibilities according to the Asset Owner - Asset Manager - Service Provider model.

The SAMP contains all the elements necessary for the corporate strategy of Unareti and Duereti to be appropriately converted into an asset management strategy. In practice, it represents the strategic guideline containing and aligning the asset management policy, corporate strategic objectives, strategies and approaches for the development and management of the asset portfolio and the asset management system as a whole.

Within this framework, KPIs are also defined for monitoring asset performance and managing risks and opportunities, integrated into asset management processes through specific procedures and periodic assessments. In addition, constant alignment is in place with the Group Enterprise Risk Management structures and with the functions responsible for Health and Safety, Environment and Quality, Procurement, Communication, Stakeholder Engagement, Organisation and HR, in order to ensure coordinated oversight of the main risk factors and implementation of the related mitigation measures.

In accordance with the SAMP guidelines, Unareti and Duereti define and implement a formal Asset Management Plan, coinciding with the companies' Development Plan and with service continuity, safety, resilience and infrastructure reliability objectives. The Plan includes intervention priorities, maintenance and renewal programmes and investment criteria. Awareness-raising and training on asset management is continuous and is based on pathways available through A2A Academy, as well as specialist initiatives included in skills development plans (e.g. master's programmes and PhDs). To support continuous improvement, the BU and the companies may use specialist consulting services to strengthen methodologies, processes and tools for managing the asset life cycle.

In terms of assurance, the asset management system is subject to periodic checks through internal and external audits in accordance with the ISO 55000 standard. Finally, it should be noted that in 2025 Unareti obtained ISO

55001 Asset Management Systems certification from an accredited body, as the first electricity and gas DSO in Italy to do so.

Business Continuity Management System

In 2019, the project for the implementation of a Business Continuity Management System was launched and, in 2022, achieved its first certification (in accordance with the ISO 22301 standard).

Since then, the scope of certified processes has expanded year after year, and today includes the following processes:

- Energy Management
- Finance
- Electricity Distribution
- Integrated Water Cycle
- Hydroelectric Generation
- IT Incident Management & Disaster Recovery
- CyberSecurity Incident Handling & Monitoring

In 2026, the extension of the certified scope to the District Heating, Waste-to-Energy and Security Control Room processes is planned.

The activities relating to the management system, as provided for by ISO 22301, are the following:

- periodic updating of the BIA (Business Impact Analysis) for all A2A Group processes. Economic, operational and compliance impacts, as well as impacts on the market and on employees, are assessed for potential interruptions over six time intervals (from 24 hours to more than one month). The BIAs also map the resources critical to the process, including the applications on which both application and infrastructure Disaster Recovery will then be built;
- periodic updating of the Risk Assessment (specific to Business Continuity) for all A2A Group processes. This is a structured analysis according to ISO 31000, in which the likelihood of occurrence of a threat is assessed (both theoretical, according to public statistics, and specific, according to events that have occurred within the A2A Group), together with the impact (inherited from the BIA) and the countermeasures in place to mitigate the inherent risk (as this is a risk on which operational mitigation is possible, residual risk is assessed).

Both the basic metrics (impact matrix and probability indexes) and the results of the BIA and RA analyses are shared with the Enterprise Risk Management structure.

Training and Awareness: both through online platforms and classroom lessons (in person or virtual);

Testing: tests of various types are organised every year (technological, process-based, hybrid technology/process, table-top);

Document review: the management system is based on a documentary framework requiring annual updating following the evolution of analyses, context and the results of tests and real events. In addition to Policies and Technical Documents, Recovery sheets are also updated; these are the files listing possible unavailability scenarios and the continuity strategies that must be initiated to mitigate/resolve them (with all characteristics in terms of recovery times and people involved);

Plant Service Continuity Assessment: an analysis is carried out on plants critical to the A2A Group to assess the level of mitigation of indirect operational risk;

Supply Chain Continuity: a process has been structured to assess the business continuity capability of critical suppliers for the A2A Group (both during tendering and ex post), in accordance both with the ISO 22301 reference standard and with the A2A Group's business continuity needs.

Within the scope of Crisis Management activities, the Business Continuity & Resilience structure provides support both during the event triage phase and in the coordination and communications required, until the adverse event is resolved and normal operations are restored. Following significant events, the necessary ex-post analyses are then carried out and any remediation initiatives are assessed.

Emergency response programme

Within the A2A Group, emergency management is entrusted to various structures: HSE, Group Security, Digital Technology & Innovation and industrial plants.

Within the Group Security Department, the following technological and organisational tools have been developed:

Security Control Room: a 24/7 operational control room in which operators monitor, through a PSIM, signals sent by fire prevention, anti-intrusion and access control systems, as well as images from more than 5,000 cameras installed at the various corporate assets. This structure is also responsible for managing emergency calls from travelling personnel and plays a central role in the Crisis Management process, receiving reports and performing initial triage, and then initiating the communication process to predefined distribution lists according to the severity of the event. A project is under way to update and redesign the Crisis Management process in line with ISO 22361.

Security Operations Center: a 24/7 operational control room in which operators monitor the technological assets (applications, network, sites) of the A2A Group. (Full description in the Cyber Defence section.)

Within the Group Security & Cyber Defence Department, various risk analyses are carried out periodically, all ISO 31000-based, one for each type of threat (physical, people, cyber). All activities, roles and responsibilities, flows and processes are regulated in dedicated procedures.

The Department's Communication, Awareness & Learning process enables the dissemination of information, good practices and knowledge of the Procedures and Policies relating to incident/emergency management activities.

Information Security

Information Security Governance

The A2A Group has implemented a structured and formalised Information Security governance model, integrated into the Internal Control and Risk Management System, with the objective of ensuring the protection of information assets, the resilience of IT and OT systems, the operational continuity of services and the overall resilience of the business.

Since 2017, the Group has structured itself with the Group Security & Cyber Defence Department, dedicated to both physical and digital Group Security, with cross-cutting responsibilities at Group level. Within it, the Cyber Defence Function defines cybersecurity policies, processes and standards to be applied in the design and delivery phases of services, according to the principles of security by design and vulnerability management.

In coordination with the Risk Prevention and Security Resilience structure, Cyber Defence:

- defines and implements the cyber risk management framework;
- ensures continuous monitoring of IT and OT risks;
- ensures periodic reporting at executive and operational level;
- identifies mitigation initiatives and monitors their implementation;
- coordinates the response to cyber incidents and threats, also through constant information exchange with the National Cybersecurity Agency.

Oversight of Information Security matters is ensured at Board of Directors level through periodic information reports to the Board of Directors of the Parent Company and to the Boards of Directors of the Subsidiaries, as well as quarterly reporting to the Control and Risk Committee within Enterprise Risk Management processes. Through structured information flows, the competent functions provide periodic updates on the cyber risk profile, the main threats and the mitigation initiatives adopted. The Board of Directors therefore receives formal and structured reports on cybersecurity and information security.

Communications on Information Security are published on the company intranet and constitute a fundamental safeguard of the governance system and of the dissemination process for the internal regulatory framework. In this context, the policies and main security documents, approved by the competent bodies of the A2A Group, including the Board of Directors for the most relevant matters, are formally communicated to all recipients in order to ensure their full knowledge and application by the organisational structures involved. Intranet communications

make the regulatory documents available, formalise their operational effective date and highlight the updates introduced, ensuring consistency with regulatory requirements and reference standards (e.g. ISO/IEC 27001, NIS2 Directive). They also constitute evidence of internal information and awareness-raising activities and contribute to ensuring the organisation's continuous alignment with the evolution of cyber risks, the related management models and the security measures adopted by the Group to protect information and technological assets.

Overall responsibility for security governance is assigned to the Group Security & Cyber Defence Department, led by Alessandro Manfredini, Head of Group Security & Cyber Defence. In the operational and specialist area, the role of Head of Cyber Defence is held by Simonetta Sabatino, with responsibility for overseeing cybersecurity matters, managing cyber risk and coordinating technical and organisational initiatives.

Security governance is based on a dedicated organisational model, structured into several specialised units overseeing cybersecurity management in both Digital and Industrial areas.

The Cyber Defence function holds overall responsibility for the information security system, defining cybersecurity policies, processes and standards, implementing the cyber risk management framework in line with the Enterprise Risk Management model and monitoring the level of security and maturity of controls. The function also ensures the performance of audit activities, coordination of the management of cyber threats and incidents, and interaction with competent authorities and external stakeholders.

Within this structure, Cyber Security Governance, Risk & Reporting oversees risk assessment and monitoring, the definition of mitigation plans, management of the regulatory framework and internal controls, as well as compliance and reporting activities.

Cyber Security Engineering & Delivery is responsible for defining technological standards, designing and implementing security solutions and overseeing the security by design process.

The Security Operations Center (SOC) structure, finally, ensures continuous threat monitoring, operational management of security incidents and threat intelligence activities.

The overall model is characterised by strong coordination with Digital Technology & Innovation structures and with the Business Units, adopting an integrated and risk-based approach covering the entire cybersecurity management cycle: from the definition of security policies and requirements, to the design and implementation of controls, through to continuous monitoring and incident response.

Information Security Policy

The A2A Group has adopted an Information Security Policy, included in an integrated system of corporate policies and procedures, accessible to all personnel via the Intranet and constantly updated on the basis of internal and external needs. These documents establish behavioural obligations, information protection principles, rules for the use of systems and credentials, and provide for formalised escalation processes enabling all employees and collaborators to promptly report security incidents, vulnerabilities or suspicious activities.

This framework is strengthened by structured information security training and awareness programmes, including periodic training pathways and simulations (for example phishing campaigns), aimed at disseminating a security culture at all organisational levels and ensuring that each individual actively contributes to cyber risk oversight.

The system complies with the relevant international standards and is ISO/IEC 27001 certified for the Information Security Management System. The Corporate Security Policy is public, while the other documents are available internally to employees.

For example, through its various corporate structures, A2A has issued:

- Policies, such as the Cyber Security Management Policy, the Enterprise Risk Management Policy, the Group Crisis Plan, the Business Continuity Plan, the Cyber Vulnerability Management Policy and Data Protection for privacy purposes.
- Procedures, such as the Security by Design Procedure, the Cyber Security Incident Handling Procedure, the Cyber Threat Intelligence Procedure and the Access & Identity Management Procedure, Procedure for managing and notifying incidents in the NIS2 area.

Through its policy and related documentation, A2A explicitly commits to:

- continuously improving information security systems, according to the principle of continuous improvement;

- ensuring the confidentiality, integrity and availability of processed data and information;
- monitoring and responding to threats to information security through dedicated Security Operations and Cyber Defence structures;
- defining individual responsibilities in Information Security for the entire workforce;
- establishing information security requirements for third parties, applied throughout the entire supply life cycle;
- guaranteeing data subjects' rights regarding personal data protection (access, rectification, erasure), in line with privacy legislation;
- implementing appropriate technical and organisational measures to protect personal and corporate data.

The A2A Group has also defined specific Information Security requirements applicable to third parties, including suppliers and partners, with the objective of mitigating risks deriving from the supply chain.

Specifically, these requirements are formalised through the inclusion of specific contractual security clauses in contracts and agreements with counterparties, as well as defined within Group policies and regulatory documents also made available through corporate tools. At the same time, A2A provides for due diligence and risk assessment processes aimed at identifying, analysing and monitoring cyber risks associated with suppliers throughout the entire life cycle of the contractual relationship. Third-party qualification and monitoring activities are based on cybersecurity criteria and include, where applicable, periodic audits and compliance checks on the most critical suppliers, in order to assess the effectiveness of the safeguards adopted and compliance with defined obligations. In addition, the Group establishes minimum security standards for all third parties accessing corporate systems, data or services, ensuring that risks deriving from suppliers, products and services are understood, recorded, prioritised, treated and monitored over time, in line with cyber risk management processes adopted at corporate level. This approach makes it possible to extend information security oversight also to third parties that process data or access the Group's systems.

According to the A2A Group documentation, corporate policies and procedures describe:

- the types of data processed (personal data, data of customers, suppliers and employees, corporate information and intellectual property);
- the purposes and methods of data use, in compliance with regulatory requirements;
- the methods for communicating and disclosing data, including rules for managing information through classification labels (public, controlled disclosure, confidential, strictly confidential);
- structured mechanisms for reporting issues relating to data protection and security (escalation channels and dedicated procedures);
- data retention practices;
- procedures for managing and notifying security incidents, also with reference to compliance matters such as NIS2, PSNC and data breach.

Information Security management programs

The A2A Group has defined and implemented a structured Information Security Management Programme, aimed at managing cyber risks and ensuring the resilience of IT and OT services, consistent with the NIST Cyber Security Framework and based on ISO/IEC 27001 requirements. This programme is aimed at maintaining cyber risk within acceptable thresholds and ensuring the operational continuity of services essential to the business, which represents a priority objective for the Group.

Service resilience is ensured through the adoption of regularly updated and tested Business Continuity and Disaster Recovery plans, supported by the presence of two Data Centers (primary and backup) and the definition of recovery objectives (RTO), as well as by the integration of the cyber component into the emergency response programme (ERP) and corporate crisis management plans. The control model also includes structured vulnerability analysis activities, cyber risk assessments in IT and OT areas, privacy analyses and impact assessments (PIA/DPIA), accompanied by internal audits on IT infrastructure and information security management systems.

For continuous oversight of technological environments, the Group relies on a dedicated Security Operations structure, responsible for continuous monitoring of IT and OT environments, cyber threat intelligence activities, vulnerability analysis and security incident management. These activities are supported by periodic exercises and tests of incident response procedures and by formalised Data Breach notification and management processes, in line with applicable legislation.

Corporate policies on information security, accessible through internal communication channels, clearly define escalation processes enabling employees and collaborators to promptly report incidents, vulnerabilities or suspicious activities, guaranteeing access to specialist support active 24 hours a day, 7 days a week through official reporting channels and dedicated procedures (for further information: A2A CERT). In particular, the Whistleblowing procedure applies to confidential reports, while the provisions of the Group policy apply to generic information security reports.

The cyber risk assessment and management process is formalised in the internal Cyber Security Risk Management policy, which describes the model adopted by the Group for the identification, analysis and treatment of information security risks. Specific risk assessments are carried out annually to support this process, the results of which are confidential. Similarly, internal and external audit activities on the Information Security Management System and related controls produce documentary evidence that cannot be disclosed, in order to protect the Group's security.

To complete technical and organisational oversight, the Group constantly promotes a security culture through communication initiatives, mandatory training programmes for figures with critical roles and periodic awareness campaigns, including phishing simulations, addressed to all internal and external personnel operating on corporate systems.

Information security oversight also extends to the supply chain through a third-party cybersecurity due diligence programme, which includes cyber qualification checklists on the supplier portal, assessments during sourcing phases and dedicated audit activities.

The A2A Group, as an additional guarantee of the achievement of corporate sustainability, strategy, security and resilience objectives, through its various corporate structures, during 2025:

- maintained ISO 27001 certification relating to the Information Security Management System;
- maintained ISO 22301 certification relating to the Business Continuity Management System.

In addition, it obtained ISO 28000:2022 – Security & Resilience certification for the Management System of Physical Security Governance Processes, as well as IEC 62443 certification with reference to industrial contexts within the PSNC compliance perimeter.

Responsible Artificial Intelligence

Artificial Intelligence Policy

A2A has adopted a policy on the responsible use of AI, structured into two complementary regulatory documents applicable to the entire A2A Group. The main contents, mapped to the requested topics, are as follows:

- Data privacy. The policy governs compliance with data privacy in the use and development of AI: it prohibits the entry into AI tools of Personal Data, Special Categories of Data and Judicial Data without prior verification and authorisation; it recalls the GDPR (EU Regulation 2016/679) – in particular the principles of Article 5 (lawfulness, fairness, transparency and data minimisation) and Article 22 on automated decision-making – and the Privacy Code. The involvement of the Compliance Privacy (COMPRI) structure is required for data protection aspects. Authorised tools must ensure data segregation on servers dedicated to the Group and located exclusively in Europe (EU Data Boundary), without data being accessible to third parties or used to train third-party systems.
- Cybersecurity. The policy protects system cybersecurity in the use and development of AI: the Cyber Defence structure is responsible for cyber risk assessment using a Security by Design and Vulnerability Assessment approach, in line with the Information Security Management Policy, the Access & Identity Management Policy and the Group Security Policy. Only authorised AI tools installed on corporate devices may be used; dedicated procedures and security measures are defined for AI systems, as well as reporting of serious incidents to the authorities.
- Bias. The policy aims to avoid potential bias (algorithmic bias) in the use and development of AI: it defines algorithmic bias as prejudice/distortion that may lead to unfair or discriminatory results, highlights the

statistical and potentially inaccurate nature of Outputs and requires critical human verification to mitigate bias and errors.

- Human in the loop. The policy keeps humans “in the loop” (human-in-the-loop) for critical decisions and always provides for human intervention: it requires the involvement of human control and prohibits use without supervision. Human “Verification” of each Output before use is mandatory (logic, consistency, correctness of data, reliability of sources, identification of errors); under no circumstances may an Output be used without Verification.
- Transparency & explainability. The policy ensures the transparency of AI systems and supports the explainability of results: each Output must include the wording “Generated with the support of Generative Artificial Intelligence” and, where possible, the documents/sources that generated it; for limited-risk systems, users must be informed of their interaction with AI and synthetic content (texts, images, audio, video) must be marked in a readable and detectable format.
- Accountability. The policy establishes clear accountability for the outcomes produced by AI models/tools: tools support but do not replace the user, who remains fully responsible for what is produced, and use of AI does not constitute an excuse for errors or inaccuracies. Roles and responsibilities are defined (Business, Digital & Innovation / Group Data Office, Cyber Defence, Legal Affairs and Compliance, COMPRI, Project Owner). Violations entail disciplinary consequences and possible criminal liability, including pursuant to Legislative Decree 231/2001.
- Clear boundaries. The policy defines clear boundaries on what AI may and may not do: it identifies permitted use cases, cases requiring authorisation by the Head of Structure (e.g. tenders, official financial documents, regulatory communications, strategic documents) and prohibited cases (e.g. recording of meetings with Legal Affairs and Compliance, Cyber Defence or Corporate Secretariat, or on sensitive topics). Only AI tools authorised and included in the Generative AI Register may be used.
- Low ecological footprint. A2A oversees the ecological footprint of data centers and AI models: it uses data centers of nearby cloud providers (in the EU), preferably powered by renewable sources, monitors CO2 emissions from its systems and experiments with proprietary and open models executed locally – with a view to AI sovereignty – on proprietary machines, with the support of Life Ventures (AI Strategy & Development).
- Prohibited systems (EU AI Act). The policy does not use/distribute systems prohibited by the AI Act: AI systems that adopt manipulative or subliminal behaviours, exploit individual vulnerabilities linked to age/disability/social condition, implement social scoring, carry out unauthorised biometric surveillance, create facial recognition databases, infer emotions in the workplace/school environment or classify people through biometric data are excluded. Applications presenting unacceptable risk cannot be purchased and, if pre-existing, must be discontinued or modified.

The policies are drafted, verified and approved at Management level: responsibility lies with the Digital Technology & Innovation Department – responsible for the governance of enterprise applications through the Group Data Office – with the support of Legal Affairs and Compliance and Group Security & Cyber Defence.

Responsible Artificial Intelligence Programs

A2A’s activities for the responsible use of AI derive from the implementation of policies 101.0008 and 101.0044 and from the “AI Act Project”, which established a dedicated Working Group and a catalogue of AI systems. With respect to the requested points:

- Limiting access to sensitive AI capabilities. Access to sensitive AI capabilities is limited: facial recognition through indiscriminate scraping and real-time remote biometric identification (facial recognition, surveillance) fall within prohibited practices and cannot be purchased/used; full access to authorised AI tools is subject to mandatory training and approval by the direct manager, Digital & Innovation and Cyber Defence, with access control (Access & Identity Management).
- Distinct labeling of AI-generated content. Distinct labelling of AI-generated content and the outcomes of AI decisions is required: the wording “Generated with the support of Generative Artificial Intelligence” must be included on each Output and synthetic content must be marked in a readable and detectable format pursuant to the AI Act.
- Mechanisms to detect/correct drift or degradation. Control systems are active that monitor model performance and generate automatic alerts in the event of model deterioration (drift/degradation). In support, the catalogue of AI systems is kept continuously updated with risk-level monitoring through a

dedicated Power BI interface and, upon release into production, consistency between the questionnaire and the system is verified, activating corrective measures in the event of a change in risk class.

- Regular assessments for fairness/bias. Models in production are subject to recurring assessments through the same performance monitoring systems with automatic alerts; moreover, Group Risk Management integrates AI risks into the risk management framework and performs updated risk assessments.
- Initiatives to lower the ecological footprint. A2A adopts initiatives to reduce the ecological footprint of data centers and AI models: use of nearby data centers preferably powered by renewable sources, monitoring of CO2 emissions from its systems and experimentation with proprietary/open models executed locally on proprietary machines (AI sovereignty), with the support of Life Ventures (AI Strategy & Development).
- Appeals process. AI systems are recorded like all corporate systems and it is possible to open specific tickets on the relevant application for reports and challenges.
- Quantification of impact on sustainability. Some AI-based initiatives have a direct impact on sustainability outcomes, particularly on waste management and recycling.
- Training of employees. Mandatory and continuous employee training is provided on the ethical and secure use of AI: introductory course on the fundamentals of Generative AI with verification questionnaires, specialist course for each authorised tool and mandatory annual refresher course; full access to tools is subject to completion of the training.

Complaint Management and Resolution Process

A2A Energia has established a structured complaint management and resolution process designed to ensure timely acknowledgment, transparent handling, and effective resolution of customer complaints. When a complaint is submitted through the company's website, customers automatically receive an acknowledgment email confirming receipt of the complaint, in compliance with applicable regulations, including information on the maximum response time (30 days). For complaints submitted via certified email (PEC), customers currently receive a delivery confirmation generated by the PEC system itself; however, a further enhancement is planned for 2026 to introduce a formal acknowledgment of receipt also for this channel. Customers can monitor the status of their complaint through the dedicated area of the website, tracking the process from initial receipt through to final resolution. In addition, the complaint management process may include direct telephone contact with customers to clarify reported issues. If a complaint is resolved beyond the service standards established by the Italian Regulatory Authority for Energy, Networks and Environment (ARERA), customers are automatically entitled to compensation, which is credited to the first available bill and communicated directly in the response to the complaint. Furthermore, the "Customer Protection – Quality Standards" section of the company's website provides information on ARERA's response standards (30 calendar days) as well as A2A Energia's average response times.

Risk management reporting

A2A's Enterprise Risk Management (ERM) framework ensures the identification, assessment, monitoring and reporting of strategic, operational and emerging risks.
Below you can find the description of the emerging risk "Structural loss of competitiveness of recycled plastics versus virgin polymers and consequent disruption of plastic recycling value chains".

Aspects	**Emerging risk**
Supporting evidence	The risk is also mentioned in the Report on operation within the section "*Risks associated with industrial and business activities*" at page 437.
Name of the emerging risk	Structural loss of competitiveness of recycled plastics versus virgin polymers and consequent disruption of plastic recycling value chains
Category	Economic
Description	Producers of packaging and other plastic products may no longer find it economically convenient to purchase recycled plastic pellets, as these are characterized by higher costs than virgin plastic. This critical issue would mainly be attributable to the sale of virgin pellets produced in non-European countries at lower prices. As a result, plastic sorting centers in Italy, including the A2A Group plants in Muggiano and Cavaglià, could experience a significant reduction in outgoing flows due to the lower use of recycled pellets in the production of packaging and other plastic products. In this scenario, sorting centers could also stop accepting plastic from separate waste collection, potentially causing a halt in upstream supply chain activities. This would occur in a period in which A2A is increasing investments in circular economy activities and aims to strengthen its leadership in waste treatment, material recovery and resource valorization, in line with the Strategic Plan 2024-2035.
Impact	A prolonged reduction in demand for recycled plastics could affect the operational and economic performance of A2A's plastic sorting facilities, including Muggiano and Cavaglià, resulting in lower revenues from material recovery activities, reduced profitability of recycling operations. In the longer term, the worst-case scenario could consist of a halt in recovery activities at A2A plastic sorting plants.
Mitigating actions	A2A continuously monitors regulatory and market developments affecting recycled material markets and actively engages with sector associations, recycling consortia (including COREPLA) and institutional stakeholders.

	Mitigation measures include: • strengthening cooperation with national consortia and public authorities to support stable end-markets for recycled materials; • monitoring the evolution of European regulations promoting recycled content and circular economy targets.

Physical climate risks for the A2A Group

Figure 1 describes the material physical climate risks for the A2A Group identified through the financial materiality assessment process carried out as part of the 2025 Sustainability Reporting. For each identified risk, the relevant business line, any associated opportunity, the time horizon over which the risk or opportunity may materialize, the description of the risk and opportunity, the type of business impact, the management strategy, and the link to the resources on which the business depends as well as its position within the value chain are indicated.
In particular, impacts on business activities and energy product sales resulting from climate change were assessed. The financial, economic and reputational assessment of physical climate risks concerns the most relevant issues emerging from climate hazard analysis and the materiality assessment.

Climate-related risks and opportunities are identified according to three time horizons:

- Short term: corresponding to the budget year;
- Medium term: from two to five years;
- Long term: beyond five years and up to 2035.

These time horizons were defined based on the analysis of the relevant climate, economic, energy and regulatory context (hereinafter referred to as scenario analysis). These definitions are consistent with the Industrial Plan, which covers a ten-year horizon (2026–2035), and with the Enterprise Risk Management methodology, which identifies and assesses risks as deviations from the objectives and forecasts set out in the Industrial Plan.

Figure 1 Physical Climate Risks

E1_1 - Generation and Trading Business Unit	
Classification and time horizon	**Classification**: Physical; Chronic **Time horizon**: Short term, Medium term, Long term
Risk/Opportunity topic	**Changes in precipitation patterns (hydraulicity)** Risks related to variations in water availability for the Group's main hydroelectric basins.
Impact	**Financial-economic risk/opportunity** Impact: lower/higher volumes and margins of hydroelectric generation.
Management strategy and investments	Development of tools designed to improve precipitation and inflow forecasts. Development of engineering analyses and models to support the scheduling of hydroelectric plants over both the medium and short term, also with the support of the Group's in-house meteorological expertise. Hydroelectric generation well distributed across the Italian territory. The Industrial Plan includes investments to optimize the use of water resources diverted for hydroelectric purposes (e.g. increased generation efficiency and pumped-storage systems).
Resources and value chain	Risks/opportunities related to water resource availability, upstream in the value chain.

E1_2 - Smart Infrastructures Business Unit	
Classification and time horizon	**Classification**: Physical; Acute **Time horizon**: Short term, Medium term, Long term **Classification**: Transition, Technology **Time horizon**: Medium term, Long term
Risk/Opportunity topic	**Resilience of electricity distribution networks** Risk of interruptions to electricity distribution service mainly caused by: *Physical causes:* - demand peaks for summer air conditioning, resulting from heatwaves; - flooding caused by intense rainfall; *Transition-related causes:* - higher energy demand resulting from the electrification of services (Data Centers, electric cars, public transport development, heating). Opportunity to make remunerated investments aimed at increasing the resilience and flexibility of electricity distribution networks.
Impact	**Reputational risk** Reputational impacts in the event of frequent or prolonged service interruptions. Penalties for failure to comply with minimum service continuity levels. Adverse outcomes in litigation initiated by parties that suffered economic damage. **Financial-economic opportunity** Remuneration of risk-management investments at a predetermined rate within the regulated ARERA business. Margins already included in the Industrial Plan forecasts.
Management strategy and investments	Working Group, in cooperation with the Municipality of Milan, to manage the effects of extreme precipitation and heatwaves. The 2026-35 Industrial Plan includes an investment programme for maintaining and developing the electricity network, enabling both adaptation to physical climate risks and the progressive electrification of energy services (heating with heat pumps, electric mobility, induction cookers, etc.), improving efficiency and reducing CO2 emissions. In particular, the plan includes measures for the reinforcement and rationalisation of networks, secondary substations and primary substations, as well as an expansion of remote asset management systems. The risk-based approach to asset management led to the achievement of ISO 55001 “Asset management systems” certification.
Resources and value chain	Risk related to energy demand peaks on the network, downstream in the value chain, in relation to issues linked to rising temperatures and service electrification. Flooding events affect the Group's own operations. Potential reputational, technical and financial-economic benefits connected to the Mindflex project, which aims to make the local distribution network more flexible in order to support the energy transition process by optimizing the use of renewable electricity generated by small local producers.

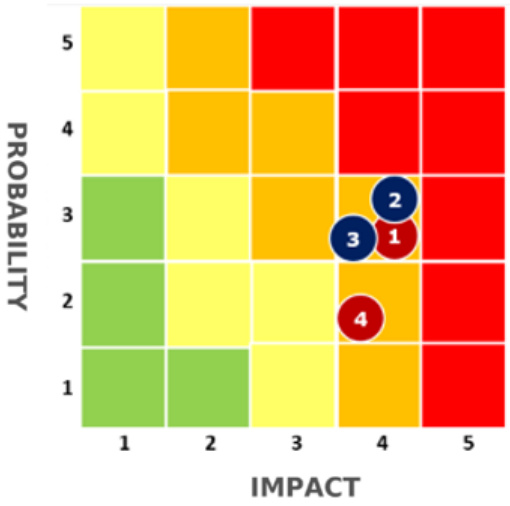
E1_3 - Circular Economy Business Unit	
Classification and time horizon	**Classification:** Physical; Chronic **Time horizon:** Short term, Medium term, Long term
Risk/Opportunity topic	**Water scarcity for drinking water uses** Risk of being unable to ensure continuous drinking water supply in the event of prolonged drought periods and/or changes in the hydrological regime.
Impact	**Reputational risk** Reputational impact in the event of interruptions to water supply service for prolonged periods and/or across significant portions of the territory.
Management strategy and investments	Mapping of losses from aqueducts in order to identify the most critical sections. Studies to use freshwater reserves (lakes), under scarcity/emergency conditions, to supplement upstream sources. Participation in the “Water Stressed Areas” project: mapping of the municipalities most at risk and refinement of the monitoring of quantities of water treated, supplied and lost. Continuous monitoring of the levels of sources and reservoirs. Emergency management using water tankers and mobile reservoirs, also with the support of Civil Protection. The Industrial Plan includes investments to: - reduce losses from the water network; - develop water abstraction from new supply sources; - interconnect aqueducts in order to create “collaboration” between supply sources and distribution networks.
Resources and value chain	Risks related to water resource availability, upstream in the value chain.

E1_4 - A2A Group	
Classification and time horizon	**Classification:** Physical, Acute **Time horizon:** Short term, Medium term, Long term
Risk/Opportunity topic	**Extreme weather phenomena** Risks for the Group's assets and for business continuity as a result of risks arising from acute physical climate hazards (floods, landslides, cloudbursts, tornadoes, hailstorms) affecting the Group's plants and infrastructure.
Impact	**Financial-economic risk** Impact: direct damage to the Group's assets and indirect damage due to the need to interrupt production activities. Reputational impacts if such extreme events were not managed optimally to ensure territorial safety in the areas under the Group's responsibility.
Management strategy and investments	Insurance contracts with coverage also extended to damage resulting from natural events. Improvement plans from a loss-prevention perspective, shared with the insurance broker. Emergency and business continuity procedures and plans to manage the occurrence of any acute weather events in a timely and optimal manner. Implementation of plant modifications aimed at preventing pollution events in the event of “cloudbursts”. Design and construction of plants (e.g. wind and photovoltaic plants) carried out taking into account the characteristics of the territory and local climatology (e.g. slope stability, windiness, etc.).
Resources and value chain	Risk affecting the Group's own operations, with consequences in terms of interruptions to essential services also downstream in the value chain.

Heatmap of physical climate risks

The reference scenarios illustrated above are considered in the analyses performed by the ERM function to identify climate-related risks, helping to provide management with insights to ensure the resilience of A2A's business model. Figure 2 below provides a summary representation, on the impact-probability heatmap, of the risks described in Figure 1. The risks were quantified based on the assumptions reported in the 2025 Report o Operations (page 154).

Figure 2 Physical climate risks heatmap



RISKS

E1_1 Hydraulicity: Changes in precipitation patterns
E1_2 Interruption of the electricity distribution service
E1_3 Water cycle - Water scarcity for drinking water uses
E1_4 Extreme weather phenomena

Level	Impact level	Probability level	(min-max)
1	Insignificant	Improbable	(0-5%)
2	Minor	Unlikely	(5-25%)
3	Significant	Possible	(25-50%)
4	Very significant	Probable	(50-75%)
5	Critical	Very probable	(75-100%)

IMPACT TYPE

Financial –economic impact Reputational impact

For financial-economic risks and opportunities, impact scales refer to average annual EBITDA impacts. Level 4 corrsponds to impacts above approximately EUR 28 million/year; level 5 corresponds to impacts above approximately EUR 76 million/year