6. GOVERNANCE

GRI 102-10
GRI 102-18

The organizational actions of 2021 have pursued the common objective of strengthening the control of Customers and consolidating the company role as technological partner of the PA, also for any perspective development of the role of National Strategic Pole.

In particular, in the Business and Technology area, Business Departments have seen the completion and refinement of the path taken in 2020 for more effective dialogue with customers, greater simplification of information flows and more precise monitoring of new business opportunities arising during the two-year period, including Sogei's direct contribution to the National Recovery and Resilience Plan (PNRR). The organisational changes were supported by market insertions functional, among other things, to adoption of the Sogei operating model in markets historically governed through high-level governance, rather than specific professional skills to support the operation of the PNRR.

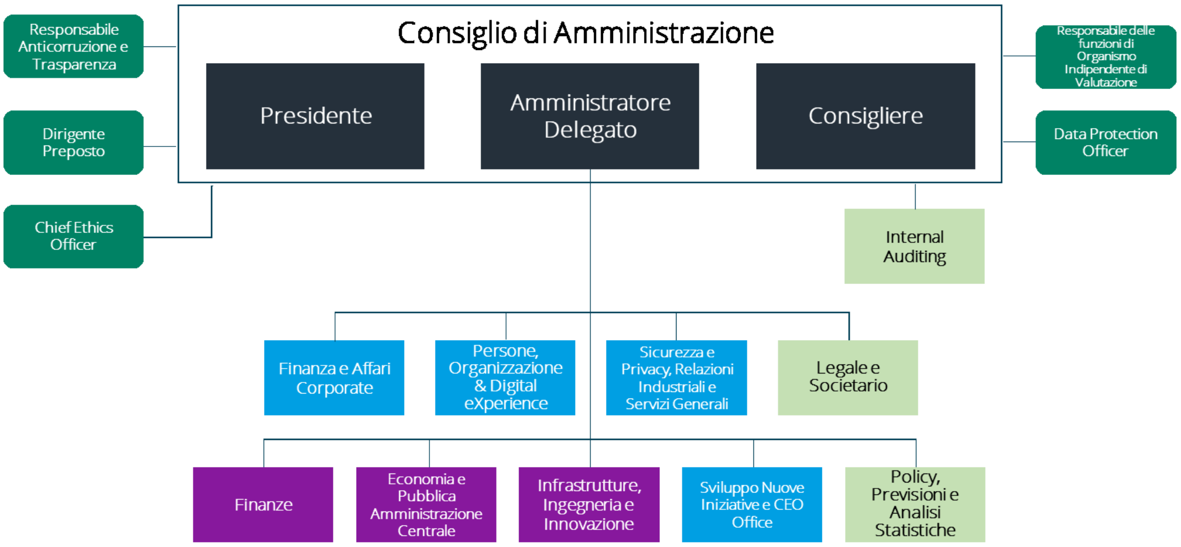
The Service & Technology Innovation Hub Management has also been thoroughly reviewed, for more effective monitoring of the issues managed and consistent with the digital transformation process of the PA through the use of cloud architectures. Completing the path taken in 2020, Management has therefore been redesigned to perimeter and segregate the traditional control and resilience of the Cloud Data Centre, within which there is also a specific area of responsibility in the Cyber Defence field and the production of services and solutions transversal to several customers; thus guaranteeing the engineering of innovation and the governance and control of the software production cycle.

In the Corporate area, organisational actions were taken to refine and consolidate the model, completing identification of specific responsibilities and marginal actions to rationalise organisational competences.

Important reorganisation was also defined in 2021 and will be operationally implemented in early 2022. In particular, actions concern the reorganisation of the Business Departments, in order to consolidate the model of direct supervision of strategic customers, with particular focus on activities resulting from the PNRR, as well as the construction of preparatory structures to strengthen Sogei's role within the National Strategic Pole.

The organisational actions planned for 2022 will also be assisted by introduction of a new Corporate Governance model, to strengthen supervision of strategic activities in an increasingly complex context.

The following diagram shows the organisational macrostructure at 31 December 2021.


Consiglio di Amministrazione
Presidente
Amministratore Delegato
Consigliere
Responsabile Anticorruzione e Trasparenza
Dirigente Preposto
Chief Ethics Officer
Responsabile delle funzioni di Organismo Indipendente di Valutazione
Data Protection Officer
Internal Auditing
Finanza e Affari Corporate
Persone, Organizzazione & Digital eXperience
Sicurezza e Privacy, Relazioni Industriali e Servizi Generali
Legale e Societario
Finanze
Economia e Pubblica Amministrazione Centrale
Infrastrutture, Ingegneria e Innovazione
Sviluppo Nuove Iniziative e CEO Office
Policy, Previsioni e Analisi Statistiche

GRI 102-3
GRI 102-4
GRI 102-16
GRI 103-1
GRI 103-2
GRI 103-3
GRI 206-1
GRI 307-1
GRI 419-1

6.1 CORPORATE GOVERNANCE

The rights of the Sogei Shareholder are exercised by the Ministry of Economy and Finance - Treasury Department - Directorate VII - Finance and privatization, in accordance with Article 5, paragraph 7, of the Prime Ministerial Decree No. 103 of 26 June 2019, as amended by Prime Ministerial Decree No. 161 of 30 September 2020, which provides for subsequent acts under the legislation in force.

According to the provisions of Article 20 of the Company's By-Laws, the Treasury Department and the Department of Finance, the latter to exercise the “similar control” due to it in relation to the in-house nature of the Company, have the right to have news and information on Company management and administration from Directors. The Shareholder and the Department of Finance verify the compliance of the social action with the directives issued and with the general annual plan as referred to in Article 26 of the By-laws. In particular, these departments must be regularly informed of the budget including the forecast and programmatic report containing the investment programmes and the annual plan. In addition, Directors must send the Finance Department the minutes of the meetings of the Board of Directors and the Board of Statutory Auditors every month, and the agenda of the meetings of the Board of Directors.

Furthermore, according to Article 26 of the Company’s By-Laws, Company management is the responsibility of the Directors, who carry out the operations needed to implement the company purpose, taking into account the guidelines received from the Department of Finance and in accordance with the provisions in the Framework Service Contract and the Agreement concluded with the Department of General Administration, Personnel and Services, in accordance with Legislative Decree No. 414 of 1997.

The Department of Finance, after hearing the other Administrations appointed for the competence profiles, provides the general guidelines concerning Company strategies, organization, economic, financial and development policies.

Corporate governance has a composite system for preventing and mitigating non-compliance risks.

In 2021, sanctions were not brought against Sogei, even non monetary ones, for non-compliance with laws and regulations, just as no legal actions were filed related to unfair competition, antitrust and monopolistic practice. There are also no sanctions of an administrative, fiscal or tax nature.

Sogei has the following secondary establishments in addition to the head office at Via Mario Carucci, 99 – 00143 Rome:

- Via Mario Carucci, 85 - 00143 Rome;
- Via Atanasio Soldati, 80 - 00155 Rome.

Sogei staff are also based at Customer premises.

Other contacts:

☎	+39 06 5025 1 (operator)
✉	protocollosogei@pec.sogei.it (Protocol's certified email address)
✉	ufficiostampa@Sogei.it (press office e-mail box)
sogei	www.Sogei.it
	https://twitter.com/@Sogei_SpA
You Tube	https://goo.gl/Jp9L6L
in	www.linkedin.com/company/Sogei
	https://www.instagram.com/Sogei_spa/?hl=it

6.1.1 ***Board of Directors***

GRI 102-22
GRI 102-23
GRI 102-24

Article 21 of the By-Law envisages that the Company be managed by a Board of Directors with three members, of which two officials from the Economic and Financial Administration and the third with functions of Chief Executive Officer, in accordance with the provisions of Article 23-quinquies of Law Decree no. 95 of 6 July 2012, converted by Law No. 135 of 7 August 2012. The By-Laws also establish that composition of the Board of Directors must ensure compliance with the laws and regulations in force concerning gender balance.

Moreover, always through Article 21, it is forbidden to pay attendance tokens, result bonuses decided after the activity and end-of-mandate payments.

Art. 27 of the By-Laws, with regard to Authorizations, establishes that the Board of Directors, after Shareholders' Meeting resolution, shall assign managerial powers to the Chairman on the matters indicated by the Shareholders' Meeting, by specifically defining its content.

6.1.2 ***Authorizations and powers conferred (TO BE UPDATED)***

GRI 102-26

The Chairman and the Chief Executive Officer hold the legal representation established pursuant to Article 29, paragraphs 1 and 2 of the By-Laws. By resolution of the Board of Directors of 13 July 2021, the Chief Executive Officer was granted the broadest powers to manage and exercise the company's signature. The Board of Directors of 13 July 2021 was informed that, until revoked, the powers of attorney already granted to Directors are in force, as well the authorizations and powers of attorney in the following areas, for example:

- appointment as Head of the Prevention and Protection Service, always in accordance with Legislative Decree No. 81/2008;
- authorization to the Security Officer, as set forth in Prime Ministerial Decree No. 22/2011;
- authorization for the Privacy area, in conformity with the European Regulation on the protection of personal data (EU) 2016/679;
- the mandate to provide the Judicial Authority and its appointees, in the context of Judicial Police investigations, and to the Organisational Structures of the Financial Administration accredited for this purpose, the findings, data and information purpose of the requested investigative activities, as undertaken by the competent Sogei departments;
- the authorization as Head of management and storage of documents processed by Sogei, on the digital storage system.

On 29 January 2020 and, subsequently, on 3 May 2021, Functions were delegated with regard to the protection of health and safety in the workplace and with regard to environmental protection and fire prevention pursuant to Legislative Decree no. 81/2008, for the various company offices.

On 29 January 2020, Head of control and coordination of all activities that may involve asbestos materials at company premises was appointed.

On 18 May 2020, the Director of Finance & Corporate Affairs was assigned special authorization, while on 29 July 2020, additions were made to the authorizations already granted to Sogei Directors.

Finally, it should be noted that during 2020, powers of attorney were granted to manage the Covid emergency period.

6.1.3 **DISCLOSURE TO THE BOARD OF DIRECTORS**

Article 27 of the By-Laws envisages that the delegated bodies must report on the general operating performance, its expected development and on significant transactions in size and characteristics carried out by Sogei and its subsidiaries. The Head of Internal Auditing reports at least once a year to the Board of Directors or to a Special Committee possibly set up within the Board.

The Manager for the Prevention of Corruption and for Transparency transmits a specific disclosure on an annual basis to the Board of Directors on the suitability and compliance of the Corruption Prevention Plan.

The Supervisory Body, the Executive Officer for Financial Reporting, the Manager for the Prevention of Corruption and for Transparency, the Manager for Functions similar to the Independent Assessment Body, the *Data Protection Officer* (DPO) and the Chief Ethics Officer also report to the Board of Directors in relation to the specific regulatory or organisational provisions.

The appointment of the Head of Prevention of Corruption and Transparency (RCPT) was renewed by the Board of Directors on 18 November 2021; the Data Protection Officer was appointed by the Board of Directors on 19 March 2018, the Head of Functions similar to the Independent Evaluation Body was appointed by the Board of Directors on 09 September 2021, while the Chief Ethics Officer was appointed by Service Order No. 4/2021.

6.1.4 **CONTROL BODY**

6.1.4.1 Similar control

Sogei is positioned on two institutional "tracks" in its relations with the MEF: with the Treasury Department as regards the framework of Shareholder's rights, and with the Department of Finance for acts of a negotiational nature, devolved and contracted in-house.

Community and national case-law clarified that this contracting is only configurable in the case where the customer entity exercises control on the contractor that is "similar" to the one exercised on its own services; thus establishing a relationship of real hierarchical and functional subordination, similar to what exists in relation to organisational structure within the institution itself.

For this reason, in April 2008, the shareholder adjusted the Company's By-Laws, limiting the powers of Directors, who carry out the necessary operations to implement the company purpose, considering the guidelines received from the Shareholders' Meeting and the Framework Services Agreement and recognizing the DF itself, as a contracting entity, the power to approve the general guidelines concerning Company strategies, organization, and economic, financial and development policies.

As of May 2010, through a series of meetings between the company's Senior Management and the Department of Finance's Fiscal Information System Directorate, the rules and operating procedures through which to implement similar control were defined according to four lines of action: powers to approve general guidelines (three-year plan, industrial plans, organisation chart, budgets and investments plan), policy-making powers, management control and control over the quality of the service rendered.

As of 1 July 2013, as a result of the incorporation of the Consip IT branch, the Department of Finance (DF) acts in liaison with the Department of General Administration, Personnel and Services (DAG) which, in turn, collects the requirements of the other Ministerial Departments concerned.

The final implementation of Similar Control in Sogei presents advantages for both the customer and the Company, since it ensures and provides certainty to the in-house relationship, based on a sharing of the definition and achievement of business objectives between Sogei and the Administration, implementing government directives.

Lastly, it should be noted that with the communication of 30 July 2019, the Department of Finance integrated the Directive on the exercise of Similar Control. This integration is designed to establish the guidelines defining the lines of industrial action and to implement the annual general plan concerning activities, investments and organisation.

6.1.4.2 Board of Statutory Auditors

Article 30 of the By-Laws provides that the Board of Statutory Auditors is composed of three statutory and two substitute members and that they remain in office for three financial years.

It also establishes that the Board of Statutory Auditors composition must comply with applicable legal and regulatory provisions concerning gender balance. Moreover, if during the term in office one or more statutory auditors should leave office, these are substituted by the substitute auditors in the order to ensure compliance with the aforesaid legal and regulatory provisions on gender balance.

It also establishes that, in addition to the provisions of Article 2399 of the Civil Code, shareholders holding qualifying or controlling stakes in electronic equipment, program and IT service production companies and suppliers, and those linked to these companies or to their subsidiaries or to the companies which control them, or those subjected to joint control by a working relationship or by an ongoing remunerated consultancy relationship or service, or by other relationships of a financial nature which compromise their independence, may not be appointed as auditors.

6.1.4.3 Independent Auditing firm

Pursuant to Article 32 of the By-Laws, accounting control is delegated to an auditor or to an independent auditing firm registered in the specific register, in accordance with the provisions of Article 2409-bis of the Italian Civil Code.

The appointment as statutory auditor, pursuant to Art. 13 of Legislative Decree no. 39 of 27 January 2010, is currently entrusted to TREVOR S.r.l., appointed by the Shareholders' Meeting of 8 June 2020 to audit the 2020-2022 three-year period.

6.1.4.4 Magistrate of the Court of Auditors

The Company is subject to the control of the Court of Auditors - Body Control Section - exercised pursuant to Article 100, paragraph 2, of the Constitution, in accordance with the procedures laid down by Article. 12 of Law No. 259 of 21 March 1958, through the Delegated Magistrate, who for this purpose attends the meetings of the Board of Directors and the Board of Auditors. Monitoring involves the Company's financial management, with a view to safeguard the public purse. The outcome of control carried out on the financial management of the Company is summarised in a resolution on an annual basis, approved by the competent Division of the Court of Auditors and sent to Chambers and to Government.

6.1.4.5 Parliamentary Supervisory Committee on the Tax Register

The remit of the Parliamentary Oversight Committee on the Tax Register, on the basis of specific legal provisions, is to monitor this Registry's operation and carry out surveys and research on the management of local tax assessment and collection services, while also monitoring the associated information systems.

6.1.4.6 Supervisory Body

The Company's Supervisory Body is tasked with monitoring adequacy in terms of effectiveness, efficiency and compliance of the two documents with the 231 Model and Code of Ethics. The Body operates on the basis of its own rules of procedure and has autonomous powers of initiative and control. It consists of three members, an external professional acting as Chairman, the Head of Internal Auditing and an external professional with considerable legal experience in the specific issues of the Body. The Supervisory Board reports to the Board of Directors and to the Board of Statutory Auditors by drafting regular reports and, whenever deemed appropriate, its Chairman reports to the Board of Directors on circumstances and significant events under its remit or on the occurrence of extraordinary situations.

6.1.4.7 Executive Officer

Within the internal control system's framework, the Executive Officer operates with the other control and supervisory boards, the corporate boards and the company departments concerned according to the interrelations, areas of operation and reporting flows defined in the "Executive Officer's Internal Regulations". By resolution of the Board of Directors of 27 March 2019, the position of Executive Officer was assigned to Cristina Barbaranelli, Manager of the Administration, Finance and Control Department, until approval of the Financial Statements for the year 2021.

6.1.4.8 Internal Auditing

The function works on the basis of the “Internal Auditing Mandate” approved by the Board of Directors of the Company on 14 September 2020. As set out in International Standard 1000 “Purpose, Powers and Responsibilities” for professional practice issued by the Institute of Internal Auditors, the Mandate is a formal document which, among others:

- defines the purpose, powers and responsibilities of internal audit;
- defines the position of the activity in the organization;
- authorizes access to data, persons and business assets that are necessary to perform tasks;
- defines the scope for internal audit activities.

The main task assigned to Internal Audit, in line with international standards, is to protect and enhance the organisation's value by providing objective, risk-based assurance, advice and expertise - also in relation to the provisions of Sogei's Organisation, Management and Control Model, through a continuous process of monitoring, evaluation and improvement of the internal control and risk management system.

6.1.5 ORGANIZATION, MANAGEMENT AND CONTROL MODEL PURSUANT TO LEGISLATIVE DECREE 231/2001 - MOG

GRI 205-1

Without new legislation on the extension of the catalogue of offences, the updating of the MOG involved alignment with the organisational changes and implementation of the changes to sensitive activities and to the internal control system; as well as the related association with the different offence families resulting from execution of theintegrated risk assessment pursuant to Legislative Decree 231/2001 and Law 190/2012. In addition, an unambiguous table linking areas at risk, associated offences, sensitive activities and reference procedures has been formalised, common to both the 231 Model and the Three-Year Corruption and Transparency Prevention Plan.

An e-learning initiative on the MOG and PTPCT addressed at all employees had been used by about 97% of staff as at the end of December 2021. Training was also provided to personnel directly involved in the application of regulations of relevance to 231*(*cybersecurity, GDPR, Legislative Decree no. 231/2001). 81/2008 etc.).

6.1.6 THREE-YEAR PLAN TO PREVENT CORRUPTION AND TRANSPARENCY - PTPCT

GRI 102-17
GRI 102-25
GRI 205-1
GRI 205-2
GRI 205-3
GOV-1
GOV-4

The PTPCT has been updated to cover the 2022-2024 three-year period. The Plan integrates and complements application of the method for managing the corruption risk introduced by the 2019 National Anti-Corruption Plan, on all business processes. In this sense, it refines the calculation method, while maintaining the evaluation approach, and completes the mapping of the internal context, started in 2020, by verticalising the structure of the strategic, methodological and finalistic principles on single processes. The operation of each Enterprise Architecture (EA) process has been described, identifying any sensitive activities at risk of corruption and associating them with the corresponding risk areas. In particular, the corruption risk management process involved the overall analysis of 68 processes and 136 sensitive activities potentially exposed to this risk.

Special emphasis was placed on the definition and planning of general measures to prevent corruption, with a focus on how to implement transparency obligations.

Always in line with the requirements of the Similar Control, the truthfulness of the non-conferability/incompatibility declarations made by the managers, pursuant to ANAC Resolution 833/2016 was verified through access to the criminal records and to the Chamber of Commerce.

During the year, activities continued to implement legislation on advertising obligations, transparency and dissemination of information by public administrations and publicly controlled companies, provided in Legislative Decree No. 33 of 14 March 2013. In this context, the "Transparent Company" section of the website is constantly updated.

During the year, training on corruption prevention and transparency was provided entirely remotely *(*e-learning or virtual classroom); an e-learning refresher course on the MOG and PTCPT was prepared for all staff. The course was attended by about 97% of the employees. Other training was provided on conflict of interest, incompatibility, non-transferability, pantouflage, integrated 231 compliance and anti-corruption in public companies, whistleblowing and transparency.

In 2021, there were no confirmed incidents of corruption.

6.1.7 ETHICS

GRI 102-17
GRI 102-25
GOV-2
GOV-3

6.1.7.1 Code of Ethics

For us at Sogei, ethics is an indispensable approach for reliability in our relations with shareholders, customers and, more generally, with the entire civil and economic context in which we operate. Ethics expresses the set of rules of conduct followed by a person. Its scope, while referring to an abstract universe of principles and values, is anything but theoretical: it concerns everyday life and translates into rules of conduct.

For this reason, in 2021, a thorough revision on the company's Code of Ethics was carried out; it regulates the set of rights, duties and responsibilities that we all expressly assume towards the stakeholders with whom we interact during our activities.

In particular, its development has pursued the following multiple objectives:

- adapt the "Tone of Voice" to make it consistent with other corporate products intended for both Sogei staff and external interlocutors;
- summarise, emphasising only the principles, values and behaviour required by limiting regulatory references to essential standards;
- update regulatory references to current standards;
- provide greater clarity and immediacy in the messages contained for increasingly effective sharing and implementation, including through examples of practical situations (what to do/what to avoid);
- integrate the principles of Digital Ethics and update behaviour with what has already been defined at Leadership Model level;
- gradually design/realise a fully digital and aesthetically more appealing product.

6.1.7.2 Digital Ethics

During the 2020-2021 period, a project was defined and launched to build the Ethical eXperience of #NoidiSogei, in order to increase ethical awareness in the organisational culture and daily execution.

The first step in this process was to become aware of the ethical practice and make it explicit through the Digital Ethics Table, i.e. the set of values and ethical principles that guide our actions, identified by listening to the experiences of top management and through analysis of the main international contributions on the subject.

In-depth analysis of the ethical issue in algorithmic systems leads to a focus on eight key thematic trends: privacy, accountability, security, transparency and “explainability”, fairness and non-discrimination, human control of technology, professional responsibility and promotion of human values.

Underlying this core set of rules, analysis of the literature mentioned above leads to a series of individual principles that the PA in general will be called upon to address as technology pervasiveness increases. All in order to maximise the benefits and minimise the possible damage of introducing artefacts (mainly AI but not only) into the production activity.

The project therefore envisages the dissemination of the proposed ethical model and its concrete adoption in the production process through a bottom-up approach achieved through Ethical Labs, i.e. through moments of co-design in order to identify requirements, best practices and actions to be followed during development of digital solutions for customers.

Prerequisite for full adoption of the model is its testing on a pilot product/service.

The increasingly pervasive use of data, IT services, technologies and Artificial Intelligence may entail ethical implications that need to be carefully assessed to support and guarantee Sogei's purpose and responsibility towards stakeholders.

The aim was to identify a Digital Ethics Model to be applied to the services provided, with particular reference to Artificial Intelligence (AI) solutions and those using Machine Learning (ML) algorithms, assigning Sogei the role of assurance of digital development based on ethical values and principles.

Digital ethics is included among the priorities of Sogei which, starting in 2019, took part in the various stages of defining the guidelines for Artificial Intelligence launched by the European Commission and started collaboration with Father Paolo Benanti, a reference figure on the international scene, in order to provide an initial framework for the ethical issue in the Sogei context. Father Benanti is a Third Order Regular Franciscan monk who has been working on ethics, bioethics and technology ethics for several years now. In particular, his studies focus on innovation management: the internet and the impact of the Digital Age, biotechnology for human enhancement and biosafety, neuroscience and neurotechnology.

This collaboration laid the foundations for defining the Ethical Experience in digital project, launched at the end of 2020, in order to increase ethical awareness in Sogei's organisational culture and daily execution.

The first step in this process was to become aware of the ethical practice and make it explicit through the #NoidiSogei Digital Ethics Table, i.e. the set of ethical values and principles that guide our actions.

The second step involved the construction, through a bottom-up approach, of an operational model applied to the production process. To this end, 4 Ethical Labs were organised, co-designing moments to identify requirements, best practices and actions to be followed during the development of digital solutions for our customers, involving about 40 people from the various organisational structures involved.

The process will continue from 2022 with the testing of the new approach on a pilot product/service, until the model is adopted in full. The evaluation of the products developed based on Ethical Quality criteria will allow us to assign Ethical badges to our services; an acknowledgement that will make the commitment undertaken and the skills consolidated by #NoidiSogei immediately visible to our customers.

Ethics in digital will be a core competence of the Sogei curriculum and will bring additional value to our customers by ensuring an important competitive advantage.

Digital ethics table

The Ethical eXperience is based on the Digital Ethics Table which accompanies the creation of products/services so that they know how to "take care" of the people who use them.

The Table, which also appears in the Code of Ethics, consists of:

- Ethical drivers: principles that give a direction to action and regulate the choice of behaviour by seeking to protect, implement and improve value;
- Ethical Values: values that contribute positively to a person's life (e.g. honesty, freedom, dignity, etc.).

The definition of the Digital Ethics Table started with a survey addressed at top management and aimed at listening to their ethical principles and values experienced in the company. In order to analyse and synthesise the results obtained, methodological steps were taken to consider not only the context of #NoidiSogei, but also the international debate on digital ethics.

Digital ethics Model

The model, designed on the basis of the results of the ongoing international debate, aims to guide reflection on the ethical implications of the services and products developed by Sogei and to identify requirements, best practices and actions to be followed during the different phases of the digital solution production process for our customers, but is scalable to further processes.

In particular, the model provides for use of checklists to stimulate reflection on ethical issues:

- Triage Checklist: in order to assess the relevance of ethical issues for a specific product/service to be developed, considering the technological choices (AI, big data, social media, blockchain, cloud, etc.), the data used and the types of users, highlighting when a subsequent in-depth analysis is needed;
- Operational checklists to be filled in while developing the product/service, in order to identify the best practices to be implemented in the different stages of the process against the only ethical issues found relevant in the previous moments.

The ethical issues considered, in line with what was defined in the Harvard study, are protection of personal data, accountability, safety and security, transparency and the ability to explain how things work, fairness and non-discrimination, loss of human control, professional responsibility and promotion of human values.

6.1.7.3 Work ethics and conflicts of interest

Over the last three years, Sogei has focused its attention on the study, diffusion and application of the work ethic. A complex topic that is addressed daily during professional activities. This process, started in 2018, with the appointment of the Chief Ethics Officer and continued in 2019 with revision and dissemination of the Code of Ethics and implementation of a process for managing conflicts of interest, in 2020, defined as its main objective to promote dissemination of the culture of ethics in the company, through seminars, forums, surveys, etc.

In 2021, Sogei created and made an IT solution available to all employees for the Conflict of Interest Management process. The purpose of putting the new application online on the intranet is to optimise the operational flow, guaranteeing the management, consultation, storage and digital protection of data, in accordance with the regulations on security and privacy.

The engineering project, started in 2020, is an opportunity for Sogei to apply and test knowledge and new methodologies inspired by Ethical eXperience, understood as the ability to create services and products with a real, positive impact on the company and civil society. The plan also includes a revision phase and updating the procedure, which will be completed in the first months of 2022 and which reflects the Sogei willingness to both apply new communication models to enhance the clarity and immediacy of information, and determination to refine and streamline those processes impacted by the transparency and corruption prevention measures provided for in the Conflict of Interest Management procedure. Following the approval phase, training will be developed and launched during 2022.

In 2021, the Ethics & Compliance Committee's assessment activity, reported regularly to the Board of Directors and to other Control Bodies, led to classification of 1 declared case of conflicts of interest, declared as "possible".

6.2 THE RISK CONTROL AND MANAGEMENT MODEL

GRI 102-11
GRI 102-15

The institutional and strategic role played, the nature and volume of data and architectures managed, the importance and size of supporting infrastructures, necessarily involve special attention for the identification and management of risks by Sogei.

The risk management process involves many players, each for its own area of competence, providing for continuous monitoring of potential risks, both on the basis of structured risk assessment methods and supporting application tools, and based on a continuous operational approach.

An integrated management model (Enterprise Risk Management, ERM) inspired by international best practices has been adopted, and involves, each for their competencies, the governance bodies, the corporate organisation, and the so-called risk specialists, i.e. those figures appointed to monitor specific risk perimeters (for example, the manager responsible for preparing the company's accounting documents who monitors administrative and accounting risks, and the Head of Prevention of Corruption and Transparency, responsible for monitoring corruption risks).

The evaluation of the main risk profiles, carried out as part of the ERM project, has led to the following main risk areas and underlying risk events.

Risk Areas	Risky events
Strategic	Top management choices with impact on strategic objectives Perception of the Company's image by customers, suppliers, public opinion and authorities Unpredictable evolution/innovation of technology and associated costs/investments Possible strengthening of socio-political or economic conditions
Operational	Customer relationships Malicious acts/accidents or force majeure Malfunctions or failures Development of application services Management of operational activities Supplier relationships
Financial Reporting	Carrying out activities and necessary fulfilment for the correct detection of business management events
Compliance	Contractual or non-contractual liabilities Violation of laws, regulations or self-regulations An event of injury or damage to Company staff, as well as potential pollution or environmental impacts attributable to the Company

For risks whose residual value is close to or exceeds the appetite threshold, a risk treatment strategy is envisaged, which may lead to mitigation through activities and/or projects which may affect the effectiveness of internal controls, transfer or acceptance of risk.

6.2.1 ENTERPRISE RISK MANAGEMENT - ERM PROJECT

During 2021, deployment of the corporate macro-risk dashboard (ERM risks) was completed. Each ERM level risk has been built by consolidating elementary risks, linked to a business process and assigned to a risk owner responsible for monitoring and updating the assessment.

In November 2021, the first ERM risk assessment campaign was launched, completely dematerialised and conducted on the new technological platform adopted (RSA Archer), by profiling specific roles, and the various players, each for its area of competence, could assess the risks, monitor them and define treatment plans.

The risk assessment campaign results are made available at op Management through a total, synthetic dashboard; all dashboards can be browsed dynamically and enable “exploding” the different graph sections into increasingly detailed views.

In parallel with completion of the ERM dashboard, in 2021, the full model was given a complete overhaul, evolving from the initial idea of a stand-alone dashboard of corporate macro-risks, with no dynamic link with the supervisory activities of all players in the control system, to a much broader system that makes ERM a true integration funnel for risk specialists.

In particular, during 2021, the workflows of the risk specialists monitoring risks in the areas of 262/05, 231/01, 190/12 and ISO-9001 will be digitised on the same technological platform as ERM.

Workflow digitisation has gone well beyond a dematerialisation *tout court*, and has led to a comprehensive review of the respective management models with a view to integration with ERM.

Specifically, all the information gathered by the various players and the evidence from the assessment campaigns, conducted by each of them in accordance with their respective competences, flow into the ERM macro-risks.

Subsequently, the functionalities for implementation of the entire cycle of Internal Audit plans and actions were also digitised in a specific workspace within the ERM platform.

In this way a federation – informative, functional and process – was created between Internal Audit and ERM to maximise the effectiveness and sustainability of governance.

In particular, all the information gathered by the risk specialists and summarised in the ERM is made available to Internal Auditing, which can thus exercise its role as "orchestrator" and "coordinator" of the internal control and risk management system more effectively and, on the other hand, can enter its own findings in the ERM, affecting the assessment of macro-risks.

6.2.2 FINANCIAL RISK MANAGEMENT

For what concerns financial risks, in particular, information on the exposure and management of financial risks related to the performance of the business is provided below.

Exchange Rate risk - The Company's business does not expose it to exchange rate risks.

Liquidity risk - Liquidity risk is managed through the availability of credit lines at banks, where the Company can always comply with the payment times laid down in the liability contracts with suppliers, regardless of the cash flow.

Interest rate risk - Revenue from sales and services and operating cash flows are substantially independent of changes in market interest rates.

Credit risk - For the activities carried out, Sogei does not have credit situations that are at solvency risk, as they relate to PA customers.

Price risk - Fees for services provided by Sogei are established contractually and subject to regular benchmark reviews. They are therefore not subject to short-term market fluctuation.

Risk related to the use of financial instruments - Sogei does not operate in the market for financial derivatives and is not exposed to this kind of risk.

6.2.3 COMPLIANCE AND RISK MANAGEMENT RELATED TO NON-COMPLIANCE WITH REGULATIONS

The main task of Integrated Compliance is to ensure, for the prevention or mitigation of regulatory non-compliance risks and related reputational impacts, the ex-ante control of corporate procedures and practices to the reference legislation of specific areas defined by Top Management, also providing support and cooperation to the corporate structures involved in each assessment, and to provide opinions and advice on compliance in the Corporate Governance field.

During 2021, implementation of the ERM and the Integrated Compliance Model development and integration project continued. It aims to ensure the confluence of elementary risks with ERM risks, with the ultimate goal of creating a digital integration model that enables moving within a perimeter consistent with the defined sustainability standards, integrating the results of assessments with ERM, in order to allow information to be shared at a consolidated level.

The new model should allow rapid interaction with ERM and be based on maximum dialogue between internal (and group) functions to achieve an integrated view of risks, as it is independent of "merely regulatory" aspects, but with a specific focus on risks that have the greatest impact on company operations (operational risk) and/or the decline in profits or capital resulting from a negative perception of the company by stakeholders, including supervisory and control authorities.

Monitoring and regulatory support continued for OIV functions which, in 2021, also carried out competence and internal cooperation controls to update data and information provided in the "Transparency" legislation and issued the certificate of conformity required by ANAC regarding the fulfilment of publication obligations pursuant to Article 1 of Law N. 190/2012.

6.3 PROCESS MANAGEMENT SYSTEMS

GRI 103-1
GRI 103-2
GRI 103-3

The Quality Management System (QMS), available in the Company since 1995, represents a governance model closely linked to the overall management of the Sogei System, inspired by the principles of efficiency, effectiveness and continuous improvement, to satisfy Customer expectations.

The QMS, based on definition of interrelated and controlled processes, constitutes, for the characteristics of non-sectorial, constant monitoring, an organizational and management tool particularly suitable for a complex business such as the Sogei one.

In 2021, with a view to fully complying with the Risk Based Thinking approach of the ISO 9001 standard, activities aimed at the integrated governance of the management system risks in the Enterprise Risk Management (ERM) model continued.

In 2021, Sogei obtained and maintained certifications for the following reference standards.

Reference standard	Scope	Certification
UNI EN ISO 9001:2015	Quality Management System (QMS)	Yes –RINA Certificate renewed November 2020
UNI EN ISO 27001:2013	Information Security Management System (ISMS)	Yes - RINA Renewal carried out on 3 and 4 June 2021
UNI EN ISO 20000-1:2018	Services Management System (SMS)	Yes - RINA Surveillance on 17 and 18 June 2021
UNI EN ISO 22301:2014	Operational Continuity Management System (OCMS)	Yes - RINA Surveillance on 17 and 18 June 2021
Guidelines for surveillance on Certified Email Administrators (V 1.0 of 18 November 2009)	Surveillance on Certified Email Administrators	Yes External audit - AgID on request Half-yearly surveillance - internal audits
Check-list for surveillance activities and certification of conformity (V.1 of 14 April 2017) for Digital Preservation	AgID surveillance and certification of conformity	Yes - AgID through RINA Maintained compliance 22 June 2021
UNI EN ISO 45001:2018 (formerly BS OHSAS 18001)	Occupational Health and Safety Management System (OHMS)	No Implemented and subject to internal audits

Reference standard	Scope	Certification
UNI EN ISO 9001:2015	Quality Management System (QMS)	Yes –RINA Certificate renewed November 2020

As reported in the layout, Sogei performed its first maintenance of the Service Management System (SGS) certification,ISO 20000-1:2018 and of the Service Continuity Management System (SGCS),ISO 22301:2014, initially defined to meet the requirements of the National Strategic Cluster.

6.3.1 DIGITISATION AND PROCESS MAPPING

Consistent with the digitisation path undertaken by Sogei, evolution of the "Process Map" in the company's enterprise Architecture (EA) continued; project was launched in order to integrate the EA with the company's Data Lake , being incorporate which will enable, through AI techniques (NLP - Natural Language Processing and Ontology Based Knowledge Management), the use of information in a more intuitive, flexible way.

In 2021, in order to build a business process representation model that allows for a multidimensional and systemic vision of the business, also in the light of market developments, a study was launched to define Sogei's "Operating Model", intended as a dynamic representation, offering different points of view, based on a product logic *(*minimum valuable product) and giving visibility to the interaction within the corporate organisation.

In 2021, application of the Lean/Lean Six Sigma methodology to business processes continued through dedicated projects.

6.3.2 CUSTOMER SATISFACTION

Listening to customer-user feedback is of crucial importance for identification of actions needed not only for the development of services offered, but also for organisational and operational improvement.

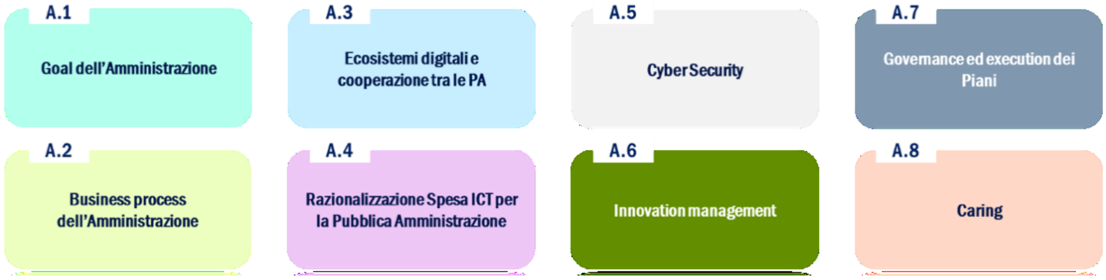
The analysis of results gathered through objective measurement of customer satisfaction makes it possible to identify the actions needed to provide products and services that are increasingly suited to their needs and expectations. For this reason, over the years Sogei has perfected a system for listening to customers/users, through adoption of a structured process to increase the quality of services offered and consolidate a climate of trust and transparency.

At the end of 2020, after a long period of time and with Top Management commitment, a project was launched to implement a Customer Satisfaction Survey campaign in 2021, in order to:

– assess the perceived satisfaction of customers and users with the SOGEI offer;

- identify, on the basis of the feedback from customers, potential areas for optimisation, evolution and extension of the current cooperation models adopted between Sogei and Administrations;

The survey, addressed at two different *clusters*, "Top Management" (customers' Top Management/Administration) and "Managerial" (customers' Business/ICTroles of responsibility/Administration) enabled investigation with Institutional Customers of some areas of the Sogei offer considered to be of higher value.


A.1
Goal dell'Amministrazione
A.3
Ecosistemi digitali e cooperazione tra le PA
A.5
CyberSecurity
A.7
Governance ed execution dei Piani
A.2
Business process dell'Amministrazione
A.4
Razionalizzazione Spesa ICT per la Pubblica Amministrazione
A.6
Innovation management
A.8
Caring

The survey was qualitative in nature and accompanied by some quantitative assessments on specific topics. It was carried out through interviews with the "Top Management" cluster and focus groups with the "Management" cluster. Analysis of results showed that Cybersecurity and Goal of Administration were Sogei's main strengths, whileInnovation Management was perceived as the area most in need of improvement. In addition, a number of specific topics were identified as significant for the future, such as data interoperability and process re-engineering.

In 2021, Sogei also supported its customer in conducting surveys on its services, in particular:

- Department of Finance, on the telematic management service of the tax process (PTT) (quantitative and qualitative survey);
- State General Accounting Office (IGIT), on the RED EVO service (quantitative survey);
- Revenue Agency, on services provided to taxpayers with disabilities (qualitative survey).

6.4 SECURITY AND DATA PROTECTION MANAGEMENT

GRI 103-1
GRI 103-2
GRI 103-3
SDP-5

Over the years, Sogei has improved its awareness that security and, more in general, the protection of information must be conceived, designed, implemented and managed, not only through structured processes and implementation of logical and physical security measures (firewall, encryption, etc.), but also through the implementation of a "Information Security &

Data Protection" governance system chaired by *a* Chief Information Security Officer (CISO), that enables the entire "security chain", to be governed and monitored.

This organization includes the role of Data Protection Officer (DPO), who plays a key role in monitoring and managing the implementation of the "General Data Protection Regulation (GDPR)" and in promoting culture in these areas.

Training is a key element for supporting information protection and the prevention of incidents and, more specifically, data breaches, and various tools have been used to achieve this, ranging from classic training with specialised teachers to the use of available social platforms. In particular, during 2021, 7 training courses were provided through collaboration platforms and 48 e-learningcourses, including 1 for new employees on the General Data Protection Regulation - GDPR. A channel was also launched on the social media platform Yammer, available to all employees, to provide information, updates and insights from the channel of the Privacy Authority and the accredited press on new Italian and European regulations concerning the processing of personal data.

The DPO continued to raise awareness through publication of thematic pills on Data Protection on the intranet and corporate social media channels.

6.4.1 COMPUTER EMERGENCY RESPONSE TEAM (CERT)

GRI 418-1
SDP-2
SDP-3
SDP-6
SDP-9

In 2021, CERT Sogei confirmed an ever-improving approach to sharing flows to and from institutional bodies involved in cybersecurity, consolidating both the management of cyber events and the implementation of the Cyber Threat Intelligence platform, focusing on customised open source tools, such as MISP, TheHive and Cortex, to fully ensure their integration into the team's consolidated processes. The public MISP instance ensured the collection of approximately 400K IoCs from the various federated entities and, consequently, initiated the various analysis processes to verify their applicability in the relevant contexts. With the TheHive and Cortex tools, automation of a large part of the security event analysis and management processes is being consolidated, and at present we are ready for an experimental phase of use in a multi-tenantconfiguration. Lastly, preliminary activities for the automatic qualification of IoCs were completed with the Sogei technical structures with which CERT cooperates on a daily basis.

The Sogei CERT continued to collaborate the with GdF (Finance Police) in the Cyber Threat Intelligence field that began in 2019, with the production of detailed intelligence reports; thanks to the help of analysis and research tools that daily detect security events on open and closed sources, reveal tactics, player techniques and reasons (threat actors*)* involved in these malicious campaigns.

In the training area, in the first months of 2021 CERT Sogei delivered, at the explicit request of the Finance Police (Guardia di Finanza GdF), an introductory course on Cyber Threat Intelligence; this course, delivered to the SOC of the GdF and divided into a theoretical and a practical part, analysed the issues related to cyber threat hunting, analysis models and contextualisation and correlation techniques needed to identify threats, using OSINT and proprietary tools.

Still in the training area, the third session of the Cybersecurity Awareness Initiative involving Revenue Agency employees was completed in the second half of 2021. The initiative aims to raise awareness about cyber threats. The next sessions will take place in 2022 and will cover all employees of the Revenue Agency.

During 2021 Sogei CERT also:

- published, using new collaboration platforms made available by the Company (in particular "Yammer"), 7 notices concerning the prevention and awareness issues in the cyber security field; therefore, the dedicated channel "Sogei CERT" has represented an important vehicle for sharing the main activities carried out daily by CERT;
- managed 4,046 events classified under different types of event/incident and divided into different areas of Constituency of Sogei CERT. In detail:
    - Cases of malware (47%): identified in emails and other malicious code vectors, addressed by activating the appropriate IT security structures for updating security and removal systems;
    - Possible threats to Sogei-managed infrastructures and services (6.4%): identified possible attack or potential exploitation of vulnerabilities (via information from CERT's intelligence sources and research activities), managed by setting up appropriate business structures to mitigate risk or solve potential vulnerability;
    - spam and phishing events (42.5%): identified, thanks also to user reports, in deceptive emails aimed at stealing the credentials of sites and services, and solved by blocking the sites linked to them;
    - events related to disclosure and leak of credentials (1.2%): these are, in almost all cases, institutional emails associated with passwords that are not related to "corporate" accounts. These credentials, filtered out from third party sites and portals not always known through successful attacks (Data breach), are collected by CERT through dedicated intelligence channels and directly communicated to the user (in the case of Sogei employee) or to the cyber security structure of the Institution involved (in the case of SIF) or CERT-MEF (in the case of the Economic Departments);

- for what concerns Sogei as Data Controller, no possible violation of personal data was detected, while in the context of Sogei as Processor, there were 11 data breaches, which were managed, solved and communicated to the Data Controllers, institutional clients of Sogei.

As part of the important, consolidated monitoring role of implementation of the Recovery Plans (PdR)[1], CERT monitored 318 PdR during 2021, of which 134 were new, and closed 60.

6.4.2 PHYSICAL SECURITY

Physical and infrastructural Security is one of the core elements of business management and has a direct impact on governance and social factors.

The security policies and measures, which ensure the protection of company assets and of the employees and external staff who man the Sogei campus 24 hours a day, 365 days a year, are in fact closely related to the impact generated by the various activities and human capital.

It is therefore essential to continuously review processes and implement security measures through a constant assessment of risks which, also in view of the particular historical period, are increasingly heterogeneous and increase in direct proportion to the consolidation of Sogei's role as a strategic partner for the Nation.

2021 further confirmed Sogei's leading role in supporting institutions in managing the emergency situation caused by the Covid-19 pandemic; thus requiring the extension of security levels both for threats arising from external factors, and to ensure compliance with health regulations and protocols as part of measures to counter the spread of the pandemic, enabling employees and suppliers to operate in full compliance with health protection.

In line with sustainability objectives, particular attention has been paid to the reconversion of some activities with a view to the impact on environmental factors through the launch of digitisation and optimisation of internal and external processes; this has already produced significant benefits, particularly with respect to paper dematerialisation and virtual e-mail traffic, with a reduction of about 40% in paper documents and 70% in e-mails.

An example of this new path is the Macars Project, developed in its initial phase during 2021. This will simplify and digitise the entire access management flow in the company for all external staff, consultants and suppliers.

[1] *The Recovery Plan is the document that in the software development cycle, downstream of a Web Application penetration Test (WAPT), is drafted and updated whenever vulnerabilities are detected on running or intended to be operated software. detailing actions planned to restore the above vulnerabilities.*

6.4.3 INFORMATION SECURITY

SDP-1
SDP-4
SDP-10

The main input of the Government system for corporate Security, therefore for integrated management of logical, physical and cybernetic security risks, is represented by the Information Security Management System (SGSI). This system enables, through a structured set of processes and specific assignment of roles and responsibilities, risk management aimed at protecting the information processed by the Company. The SGSI continues to evolve to meet company security requirements and the security requirements of national law. With this in mind, the main activities carried out in 2021 concerned:

- the revision of the risk management methodology for integration with the Business Impact Analysis performed on services;
- conducting audits and assessments for information security handled by critical ICT services. During the year, 6 audits and 1 assessment were carried out in compliance with AGID regulations;
- updating company security policies in accordance with new IT security requirements to which the Company is subject;
- monitoring IT security indicators and risk treatment plans defined as a result of audits and assessments. In the area of information security, data protection and business continuity, 23 return plans have been opened and 5 have been closed.

6.4.4 OPERATIONAL CONTINUITY

In 2021, maintenance of the certificate of conformity to the ISO 22301:2014 reference standard of the Business Continuity Management System (BMS) was confirmed. The Business impact Analysis methodology was reviewed, to identify continuity parameters and critical resources, and integrated in the Risk Analysis methodology, in use in both the SGSI and SGCO context.

The Business Continuity Plan has been generalised and extended to the services considered most critical, even if not currently included in the scope of application of the ISO22301 certificate, and integration of the above-mentioned Plan with the Disaster Recovery Plan was finalised

In 2022, the plan is to extend the scope of the SGCO to include additional critical services and to expand crisis scenario testing activities.

6.4.5 CLASSIFIED INFORMATION

SDP-7

Sogei implements a Management System of Classified Information (SGIC, Sistema di Gestione delle Informazioni Classificate) that collects and harmonizes the different procedures dedicated mainly to personnel with security authorization. Together with the SGIC, Sogei works and operates through a security area responsible for managing classified information in accordance with the State Secret regulations. The area is managed by a specific structure, managed by the Security Officer, with the support of other company figures, according to the different operative profiles of the Sogei's main Security Secretariat.

All operational areas of the main Security Secretariat, including the CIS infrastructure ”Communication and Information System Security, formerly the EAD Area), are recognized by specific provision by the Presidency of the Council of Ministers – DIS and approved by the UCSE to process data and documentation with classification of secrecy and qualification of security up to Secret (S) – NATO EU/S.

In 2021, classified documentation processed by the main Security Secretariat on a special classified protocol register amounted to 100 incoming requests and 104 outbound requests.

6.4.6 PROTECTED DATA

SDP-8

Sogei receives requests from the Judicial Authorities and Institutional Customers concerning the retrieval of transactions relating to one or more subjects (natural and legal persons) recorded in the Fiscal Information System in relation to ongoing inquiries, investigations, assessments and audits.

These requests of a confidential nature, considered as "protected data" and registered in a special Protocol application register, particularly relate to:

- the timely or massive extraction of information on taxpayers registered in the FIS databases;
- the tracking of operations on the access and use of IT services carried out by FIS users and recorded in the log archives;
- the extraction of tracking information for email and internet browsing;
- the tracking of invoice payments by the Public Administration by monitoring the Commercial Credits Platform;
- the tracking of access to the NoiPA system;
- the timely or massive extraction of information/documents on one or more citizens registered on the NoiPA system database:
- extraction of Greenpass information;
- extraction of information on the "support" decrees;
- extraction of "Bonus" information.

In 2021, 1,487 incoming requests received at the PEC of protected data and 2,066 outgoing replies via the same PEC were registered.

6.4.7 DATA PROTECTION

In the context of EU Regulation no. 2016/679 (GDPR) and the partially-amended Privacy Code (Legislative Decree no. 196 of 30 June 2003), Sogei operates as Data Controller in the processing of personal data carried out in the corporate context. By virtue of designation granted by the Authorities who are Data Controllers, Sogei operates as Data Processor in relation to the services performed on behalf of these Administrations.

Applying the accountability principle defined by the GDPR itself, the company has adopted a Privacy Management System (SGP) that is divided into an organisational model with roles, responsibilities and division of tasks between the various structures with respect to the processing of personal data and the obligations imposed by the legislation, with a view to simplifying, effective and efficient organisation. The SGP applies to Sogei in its dual role as the party responsible for the computerised components of the Administrations' processing operations and as the controller of the processing operations it carries out for its own corporate functions.

The main activities carried out in 2021 concerned:

- the updating, integration and drafting of documents within the SGP *(*policies, guidelines and procedures) for the transposition of new regulatory dictates at national and European level, the pronouncements of the Italian Data Protection Authority and the EDPB *(*European Data Protection Board);
- computerisation of the management of privacy obligations on the processing of personal data, carried out on behalf of Administrations or for corporate purposes, to make it easier to carry out and keep a record of it;
- revision of the process for the designation of providers as processors/sub-processors under the European Commission Decisions of 4 June 2021 on standard contractual clauses between controllers and processors (Decision (EU) 2021/915) and on the transfer of personal data to third countries (Decision (EU) 2021/914);
- information/awareness-raising of employees on data protection issues;
- training dedicated to corporate structures on the methods adopted by the company, in agreement with the Administrations, for personal data protection and impact assessment;
- supporting the controller Administrations in carrying out privacy obligations on personal data processing;

Sogei also periodically carries out controls aimed at improving awareness of the obligations provided for in legislation and checking their implementation.

The following audits were carried out in 2021:

- assessment to check the terms and criteria inherent in data retention times for corporate processing, with assessment of any gaps and definition of related remedial plans;
- assessment on all computer services that process personal data;
- audits and self-assessment and of some suppliers;
- audits of system administrators in specific areas;
- vertical audits of certain IT services provided on behalf of administrations.

6.5 IT GOVERNANCE

GRI 102-2
GRI 103-1
GRI 103-2
GRI 103-3

In these pandemic months, Sogei has begun to rethink its way of working in order to be able to respond quickly and efficiently to the needs of citizens and the country; considering its experience during the first period of emergency and keeping "an eye" on what the recovery, thanks also to the use of funds made available by the PNRR, might entail in terms of the need for digital applications that favour the transformation of PA.

We have reflected deeply on what happened in order to transform the emergency situation into a useful opportunity for change, to be exploited today and, above all, in the future and a plausible scenario of growth, working on the improvement of production models, methodologies, metrics and tools used in the production process.

6.5.1 NEW MODEL PMO

Sogei's renewed mission as a strategic partner of the PA in the country's path to innovation and digitisation requires an evolution of the PMO's strategic role.

The increase in the number of Public Administrations "served" highlights the need for the company to always have an "overview" of its operations in order to continuously verify its ability to act within a model of overall consistency that ensures compliance with efficiency and effectiveness parameters.

During the year, the model of a "New Sogei PMO" was designed and partly implemented, taking into account the new challenges to be faced, on the basis of what emerged from interviews with the heads of the organisational structures, without neglecting methodological and market elements.

The expectation is for a PMO that has an integrated and centralised view of all projects, their time and cost dimensions as well as a central role as an enabler of business integration and a facilitator for decision making.

6.5.2 INDUSTRIAL MODEL

During 2021, the new Industrial Governance Model was designed, building on the experience of applying the Operating Model in previous years.

While the main objective of the Operating Model developed in 2020 was to provide data and information to guide Sogei choices and decisions in view of the strategies dictated by Top Management, the "Industrial Governance Model" project developed in 2021 had more ambitious aims, since it set itself the objective of defining an operational framework of industrial governance for the objective assessment of the industrial sustainability of new contracts/projects and for the analysis of the model implemented by the company with respect to the expected industrial model.

The industrial elements considered are:

- service and delivery models adopted;
- onboarding strategies and models;
- internal and external value created and expected industrial performance;
- mapping and defining strategies to mitigate and monitor specific risks;
- operational sustainability of the contract/project from the point of view of skills needed, time, goods/services for the start and execution of the contract/project.

Once the model is consolidated, IT tools will be developed to facilitate its application.

6.5.3 PRODUCTION GOVERNANCE

In the development process in 2021, the Agile and DevSecOps approach started to be applied on projects of a certain complexity, in which Agile Scaling practices were implemented due to the need to coordinate the work of several Scrum teams.

On this occasion too, the shift-left paradigm was also tested for security aspects, identifying a security champion who, from a DevSecOps perspective, was able to anticipate potential vulnerability analyses as early as possible, optimising the time needed to pass the final penetration tests. Additional tools for automating dynamic security tests were also provided.

6.5.3.1 Metrics of software development

The in-house competence centre has consolidated its collaboration with GUFPI and IFPUG by sharing its experience and solutions at several national and international conferences. In particular, Sogei's involvement in the IFPUG continued on the work of two groups dealing with methodological developments:

- Functional Sizing Standards Committee;

– Non-Functional Sizing Standards Committee.

Once again this year, this important work has enabled the Sogei CFPS/CFPP certificate community to stay abreast of methodological developments on the market and to be able to contribute to the decision-making dynamics that determine them.

In particular, the last year has seen the definition of strategies for using the outputs of some of the experiments launched in previous years, such as SNAP and PFS. In specific contexts, definition of these strategies has led to a real industrial application, and in fact thanks to the definition of a "fast" mode for measurement of non-functional based on SNAP we can proceed, for example, to a broad and relatively inexpensive assessment of this part of the measurement of software products.

The novelty of the last months of the year is Sogei's role as Chair of the Non-Functional Sizing Standards Committee, which guarantees a very high level of control of non-functional sizing methodologies. The possibility to take part in the governance of method evolutions is especially important at a time when non-functional measurement is being introduced in various contractual contexts and when interest in quality measurement is, in general, keenly felt both in the PA and in relations with suppliers.

The internal competence centre continued to independently deliver the courses for preparation of CFPS/CFPP certification aimed at keeping the number of certifications high and spreading the culture of measurement throughout the company, ensuring an increase in the quality of counts and the level of supervision of outsourced activities.

The new version of the company's software measurement tool enabled the parallel use of FPs and SFPs. Work has also started on integrating all databases containing measurement data into this new product.

6.6 MANAGEMENT OF OFFERS

6.6.1 SERVICE CATALOGUE

It is the business process support tool that surveys the Services for the PA, providing them with information and attributes that characterise their technical, functional and security aspects.

During the year, the Catalogue was of particular interest for a number of strategic projects in the Security Government & Data Protection area. In addition to the normal activities of application assistance, methodological support for modelling and internal training on specific areas of interest, and the typical data recovery and reclamation initiatives, the entire period was characterised by developments that added important functionalities to the tool:

- GDPR: the Security and Privacy Measures documents of the ICT Service have been further customised according to the Data Controller Customer; the criteria for calculating the Residual Risk has been improved; the version of the FOURSec Security Measures master file has been updated;
- BIA: as part of the Business Impact Analysis (BIA), the criterion for calculating the Recovery Time Objective (RTO) index applied to each ICT Service was improved, making its value automatic rather than discretionary.

The ICT Services were enriched with information on their infrastructure component from the Configuration *Management Data* Base (CMDB);

Finally, the federation with the CMDB was strengthened by redesigning the interchange interfaces to improve the quality and completeness of the information content transmitted.

With a view to continuous control and monitoring of contents, during the year an assessment of the Technical Services was launched to rationalise the entire register.

6.7 PARTICIPATION AND ASSOCIATIONS

GRI 102-13

Membership of the associations allows the Company and its employees to take advantage of the services provided by them, in terms of publications, updates and in-depth analysis on the regulations, training and information seminars, collaborations and comparisons needed and instrumental to carrying out its institutional activities.

The main aims of identifying associations of interest can be summarized as follows:

- to promote the exchange of information and updating on new technological and management trends;
- to guarantee professional updating in the technological and management spheres in order to optimise the support processes for the customer and the company;
- to focus on particularly sensitive areas (gender equality, ethical and social sustainability, security, privacy, etc.).

Joining the associations follows the *"Guidelines and criteria for approval of membership of Associations, Bodies, Foundations and Committees"* which foresee a process of gathering needs and approval when the following criteria for requirement assessment are assessed:

- INHERENCE - The aims of the association and benefits that can be achieved must be relevant with respect to the activities and services provided by Sogei to institutional clients and for their business operating needs.

- INTEREST - Membership of an association must satisfy a true need for belonging to an "association" context.
- PROFESSIONAL NEED - To guarantee the development and professional updating of employees and to maintain/renew any professional certifications acquired.
- SPECIFICITY - To be understood in terms of verification and evaluation of the particular (or “original”) “characteristics/competences” or in any case of other specific elements of the Association to be joined and which justify the “choice”, as an alternative to others which may be active in the same context. In cases where there has not been a preliminary verification/attestation of the “specificity” requirement, identification of the beneficiary of the membership fee may take place after comparative assessment of the interested parties which, following a public notice with an indication of the research and assessment criteria, have expressed an interest in submitting their application.
- COST/BENEFIT RATIO - Expenditure for payment of the membership fee must be proportional to the benefits obtained also considering the cost to be incurred for purchasing the services provided in case of not participating in the association.

In 2021, Sogei joined the following associations:

Scope	Association
ICT	ITALIAN ASSOCIATION FOR INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) DAMA ITALY CHAPTER GALILEO SERVICES GUFPI-ISMA IFPUG ISACA INTERNATIONAL PROMETEIA S.P.A RTCM UNINFO XBRL ITALIA
Corporate and *Governance*	ASSIDIM ANDAF ANRA AODV 231 - ASSOCIAZIONE DEI COMPONENTI DEGLI ORGANISMI DI VIGILANZA (ASSOCIATION OF MEMBERS OF SUPERVISORY BODIES) ASSOCIAZIONE ITALIANA INTERNAL AUDITORS (ITALIAN INTERNAL AUDITORS ASSOCIATION) ASSONIME ASSOCIAZIONE FRA LE SOCIETA' ITALIANE PER AZIONI (ASSOCIATION OF ITALIAN STOCK COMPANIES) ASTRID SERVIZI S.R.L. CSR MANAGER NETWORK

Scope	Association
	UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE DI ROMA (NDUSTRIAL ENTITIES AND ENTERPRISES OF ROME)
Staff	AIF ASSOCIAZIONE ITALIA FORMATORI (ITALIAN TRAINERS ASSOCIATION) ASSOCIAZIONE ITALIANA PER LA DIREZIONE DEL PERSONALE (ITALIAN PERSONNEL MANAGEMENT ASSOCIATION) FERPI - FEDERAZIONE RELAZIONI PUBBLICHE ITALIANA (ITALIAN PUBLIC RELATIONS ASSOCIATION) HRC INTERNATIONAL ACADEMY ICF ITALIA INTERNATIONAL COACH FEDERATION ISTITUTO ITALIANO DI PROJECT MANAGEMENT (ITALIAN INSTITUTE OF PROJECT MANAGEMENT) VALORE D
Security	AIIC - Associazione Italiana Esperti in Infrastrutture Critiche (Italian Association of Experts in critical Infrastructure) A.I.P.S.A. - ITALIAN ASSOCIATION OF SECURITY PROFESSIONALS CLUSIT - ASSOCIATION FOR IT SECURITY ECSO - EUROPEAN CYBER SECURITY ORGANIZATION ISFA ITALIAN CHAPTER