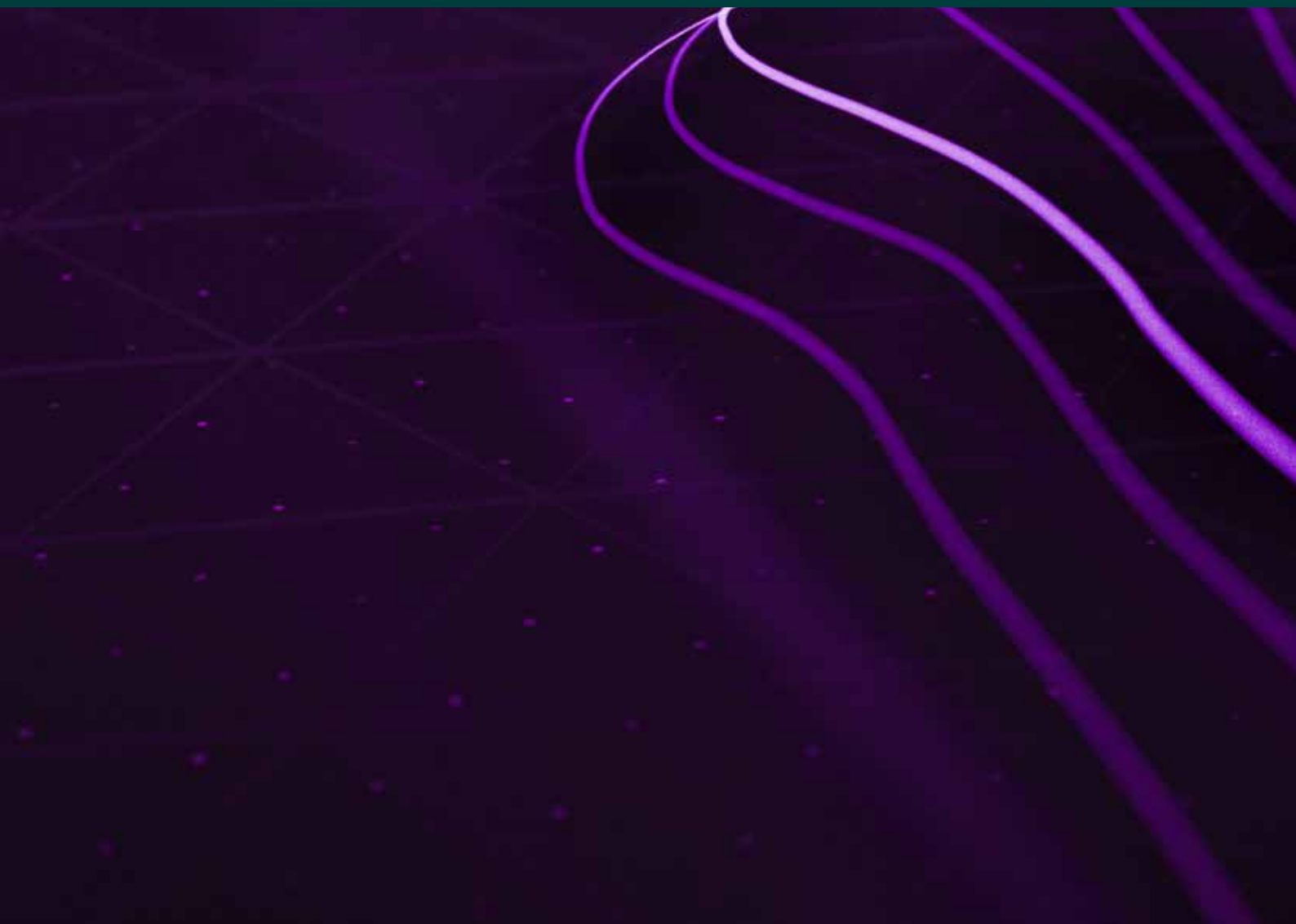
Business Ethics

- Business Integrity
- Data Ethics
- Security
- Responsible supply chain management



An ethical approach to business

At Sisal we believe in an ethical approach to business, in a set of behaviours and values that determine an individual's conduct within and towards the community.

Sisal's conception of Business Ethics rests on three pillars:

1. **Business Integrity:** meaning the way Sisal and its employees act, which is in compliance with the law and regulations and inspired by the principles of **legality, loyalty, fairness, transparency** and **responsibility**.
2. **Data Ethics:** meaning the adoption of fair and honest practices in terms of procedures, types and purposes of personal data collection and processing, as well as maximum transparency in dealing with our customers.
3. **Security:** meaning respect for the **confidentiality, integrity** and **availability** of **IT infrastructure** and **systems**.

Business Ethics Week

Every year, Sisal organises a **Business Ethics Week** (in 2022 entitled "**We Are Aware**") featuring compliance training and awareness raising initiatives. Activities include the organisation of **gamification initiatives, theme quizzes and webinars** aimed at the entire corporate population. The 2022 Business Ethics Week focused on privacy and data ethics, whistleblowing and the Code of Ethics, information security, HSE and relative ISO certifications, anti-corruption and conflict of interest. 98% of respondents to the event survey said they found the initiative useful and effective, while 89% said they had felt engaged throughout the week. The initiative was also successful in terms of the access rate to the daily posts (58% of the company population) and high participation in the webinars.

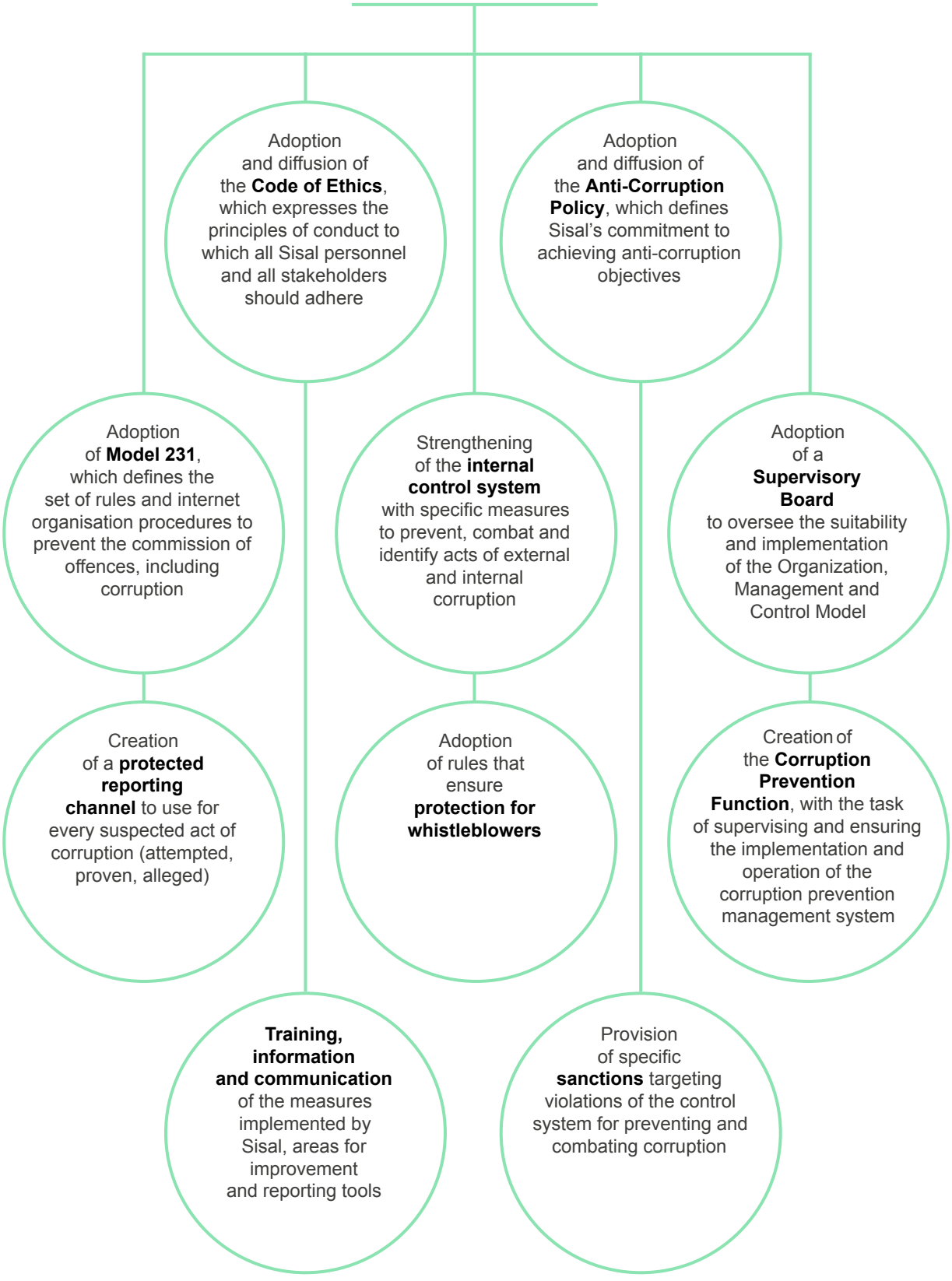
Business Integrity

Combating Corruption

In full compliance with the law, regulations and all the provisions of international standards and guidelines, Sisal Group is committed to preventing and combating the occurrence of offences in the conduct of its activities and has adopted business integrity as one of its primary values, through which it sends out messages of loyalty, fairness, transparency, honesty and integrity.

In this context, corruption is an intolerable obstacle, so we are duty bound to actively contribute to the fight against corruption and conflict of interest. To this end, Sisal has put in place a set of rules, models, checks and training and communication measures.

Models and tools



All Sisal people are responsible for complying with anti-corruption law: all employees are therefore constantly involved in **training and communication initiatives**, and all the relevant documents are easy to access via the company's website and intranet portal.

Sisal is also the first company in the gaming industry in Italy to have obtained **ISO 37001:2016 certification (anti-bribery management systems)**, which is designed to mitigate risk relating to corruption (active or passive, attempted or committed, public or private). This certification is issued by an independent third party and identifies a management standard to help organisations combat corruption by fostering a culture of integrity, transparency and conformity. Under its corruption prevention management system, Sisal employs **specific instruments** that have been upgraded (such as due diligence) or newly introduced to satisfy legal requirements (such as the Corruption Prevention Conformity function). All this testifies to and strengthens the **internal control system**, ensuring it is in a position to manage and limit the risk of "mismanagement", which not only causes economic harm, but also and more importantly damages the company's reputation. People engaged in activities that are sensitive and exposed to significant risks are identified and given special training.

Conflict of interest management

Conflict of interest means any situation in which there is a conflict between the expectations, interests or advantages of an individual (e.g. an employee) on one hand and the expectations, interests or advantages of Sisal on the other, which may affect the individual's capacity to make decisions and carry out their tasks impartially and effectively.

Sisal has policies and procedures in place to guarantee the communication, identification, management and monitoring of conflicts of interest, whether potential or actual.

In this context, Sisal:

- has a Corruption Prevention Conformity Function (CPCF) which also monitors, records and manages conflicts of interest, as well as reporting any critical conflicts of interest identified to the CEO;
- provides instructions to all those who have relations with the company (such as members of the board of directors, board of statutory auditors and supervisory board, all employees whether on open-ended or fixed-term contracts, interns, temporary personnel and similar and third parties in general in negotiation relationships) on how to follow the company's procedures for reporting any situation which may, even only potentially, generate a conflict of interest, mitigating the situation of an identified conflict and/or signalling any inadequacy in Sisal's procedures in this area.

Respect for human rights and non-discrimination

Sisal has adopted a **Human Rights & Anti-Discrimination Policy** in line with major international agreements such as the Universal Declaration of Human Rights, the International Labour Organization's declaration on fundamental principles and rights at work and the principles of the UN Global Compact. Sisal's policy applies to all its employees, regardless of country and contract.

We advocate the **principles of diversity, equity and inclusion** and the **right to working conditions that respect** the individual and their dignity, guaranteeing:

- basic human rights, a minimum and fair salary, sustainable working hours and conditions, full access to workplaces and tools, exclusion of underage labour (by checking age before hiring) and forced labour;
- the physical and psychological integrity and individuality of all persons;

- exclusion of all forms of behaviour entailing harassment or discrimination regarding gender, age, disability, nationality, sexual orientation, ethnic background, religion, political opinions and any other forms of individual diversity;
- freedom of expression, the right to participate in organisations that defend and advocate the interests of the individual, and the right to representation by trade unions or other bodies elected in compliance with current law and practice in the various countries in which we operate.

To this end we have special listening channels in place, from whistleblowing and grievance mechanisms to **periodical surveys** (DE&I, NPE, Culture), but we are in any case aware that the absence of whistleblowing reports does not mean there are no potential problems and we therefore work proactively to anticipate specific needs and risk situations.

Whistleblowing

The management and **all Sisal employees are encouraged and obliged** to report any behaviour, including omission, that is or might be an **infringement or incitement to infringe laws and regulations or the values and principles set out in Sisal's Code of Ethics and Conduct, Model 231 and policies and procedures**.

All Sisal personnel receive specific training and regular updates on what can be reported and through which channels. Employees and external subjects can also use **Speak Up!**, a whistleblowing platform available in all the languages spoken in the Group[33] and managed by a third party organisation to ensure independence.

Further, to strengthen trust and participation in the fight against illegal conduct, Sisal makes it **possible to report** behaviours associated with **internal fraud, mistreatment of employees** (e.g. discrimination, mobbing, harassment, retaliation), **occupational health and safety irregularities, bribery, conflict of interest, falsification of documents, misuse of company assets** (e.g. illicit use of company assets or information) or **breaches of privacy, IT security**, fiscal integrity of the organisation, etc[34].

Whatever whistleblowing channel is used, the **identities of the reporting and reported parties are always guaranteed protection and confidentiality** by processing their data in accordance with the law and any other useful measures adopted. **Sisal accepts anonymous reports**.

At the same time, Sisal forbids and punishes acts of retaliation or discrimination against the whistleblower, whether direct or indirect, for any reasons directly or indirectly connected with the whistleblowing.

In 2022, Sisal received 47 reports, of which 4 relevant to legislative decree 231 (mainly infringement of the Code of Ethics and company procedures – 2 closed and 2 still ongoing). There were 44 signed reports (sent to 3 whistleblowing addresses) and 3 anonymous ones on the new platform. Only one report led to disciplinary proceedings against Sisal employees.

[33] The platform is available via the following link: https://sisal.integrityline.com/frontpage.Reports may also be sent by post to: "Servizio Segnalazioni" Via Ugo Bassi, 6 - 20159 Milano.
[34] Reports will not be considered if found to be false, either deliberately or through gross negligence, groundless and/or submitted for the sole purpose of harming the reported party or referring to situations of an exclusively personal nature and beyond the bounds of the law. In more serious cases (e.g. a deliberately false report), the whistleblower's conduct may lead to disciplinary proceedings.

Combating money laundering and the funding of terrorism

Ensuring effective and timely monitoring of the adequacy of its systems for preventing and combating illegal gaming, money laundering and funding of terrorism is a priority at Sisal. That is why it has a comprehensive system of policies and procedures in place for the entire Group. The **Group policy** defines the structure and organisation of the Group Anti-Money Laundering Function and its responsibilities, roles and tasks, as well as the general rules that all the Italian companies and foreign subsidiaries must comply with in order to prevent money laundering and funding of terrorism. The Policy is then articulated in **individual procedures and operating instructions** specific to the various separate entities, also with regard to national characteristics and requisites.

In line with the **risk-based approach** and to fulfil the relevant legal obligations, Sisal carries out **adequate monitoring using automated systems developed in-house on the basis of industry-specific know-how and databases provided by external providers**. Such systems make it possible, among other things, to carry out thorough **reputational screening** of players and the ownerships of retail network operating companies in order to verify the **existence of the legal reputational requisites**, both prior to contract stipulation and regularly thereafter.

Transaction monitoring, customer profiling and documentation retention activities are carried out **using systems developed in-house and customised for the peculiar needs of the gaming world**. The **Transaction Monitoring** tool enables us to monitor gaming operations for the purpose of identifying movements to flag and, where necessary, initiating the process of reporting the suspect transaction to the authorities.

Training is indispensable in the internal control system and **obligatory for all employees** (including new hires) and **collaborators, including point-of-sale staff**, to raise their **awareness of ML/FT** risks and extend their basic knowledge of **anti-money laundering law**, given that they are already familiar with the internal procedures and know how to recognise and deal with potential suspect transactions or activities.

Data Ethics

Alongside the definition of the purposes and procedures for the processing of personal data, Sisal has adopted a series of **Data Ethics** principles in support of an ethical decision-making process. In particular, Sisal prioritises and guarantees respect for such values by applying the following principles:

- **Accountability:** Sisal has adopted a governance model to monitor control activities, commitment and responsibilities and to strengthen the ethics, conformity and sustainability of services, which are always designed and implemented in compliance with applicable regulatory requirements, using a privacy by design approach to guarantee personal data protection.
- **Ethics & Fairness:** Sisal adopts fair and equitable practices towards customers, with the objective of minimising discrimination and treatment that is penalising or biased.
- **Privacy:** Sisal processes customers' personal data in accordance with privacy principles and legislation and guarantees data minimisation, retention for limited periods, use for specific and transparent purposes and accessibility at any time.
- **Quality & Accuracy:** Sisal aims at a high level of data quality in terms of accuracy, precision and updating and adopts all the necessary measures to enable deletion or prompt rectification.
- **Transparency:** Sisal guarantees a high level of transparency and clarity regarding the procedures, types and purposes of personal data collection and processing on channels, products and services provided to customers.
- **Responsible Data Sharing:** Sisal guarantees that technical and organisational measures are in place to ensure legal compliance and also protect personal data processed by third parties acting in the name and on behalf of Sisal.

In line with its declared Data Ethics principles, Sisal has adopted a specific privacy protection policy based on three main lines of action:

Eminence & Strategy	Privacy & Accountability	Responsible Data Sharing
Awareness and training: special activities are organised at least annually to heighten the awareness of employees and third parties around data protection issues, implement a diffuse compliance model and guarantee correct management of business processes in terms of Privacy and Data Ethics. **Control framework:** continuous monitoring by means of second level controls on the aforementioned general Privacy & Data Ethics principles (legality, transparency, correctness, data minimisation, limited retention, data controller accountability). **Transparency:** drafting of information notices and public pages illustrating Sisal Group's commitment and mission regarding Privacy and Data Ethics and effective management of data subjects' requests to exercise their rights. **Cookie management e cookie compliance:** Sisal has implemented a process for monitoring compliance with current law on cookies by Sisal's websites and mobile app.	**Governance Model:** Governance Model: Sisal has adopted an internal governance model that provides a comprehensive control structure guaranteeing protection of personal data specific to business activities and identifying the roles and responsibilities of subjects involved in guaranteeing that personal data are processed in compliance with applicable laws (first and foremost, EU Regulation 2016/679 (GDPR)), thereby improving the company's commitment and awareness in this area. A Data Protection Officer (DPO) has also been appointed to provide consulting to the Data Controller, also in relation to the assessment of impact on data protection, and ensure that internal processes are aligned with current personal data processing legislation. **Policy and procedures:** to guarantee compliance with the relevant provisions of privacy law, Sisal has drawn up and regularly updates its Privacy & Data Ethics policy and procedures. **Processing Register:** the process that updates and monitors the processing register is managed in such a way as to guarantee tracking of Sisal's activities involving the personal data processed. **Exercising of data subjects' rights:** Sisal has defined a process for receiving and promptly responding to data subjects' requests to exercise their rights. **Privacy by design and by default:** Sisal uses a checklist to assess privacy protection "by design" and "by default" in the case of new initiatives, services or products. **Data Protection Impact Analysis:** Sisal has adopted a risk analysis and impact assessment methodology for types of processing that entail a high level of risk for data subjects' rights and freedoms, in line with the methods adopted by the company and with the definition of security measures to reduce such risk.	**Third-party contract management:** management of third parties involved in processing personal data, including drafting and negotiation of privacy clauses in contracts and of data protection agreements, as well as verification of guarantees provided by the third party. **Monitoring of third parties:** continuous monitoring of third parties' level of privacy compliance by means of periodical audits of selected stakeholders that process personal data for Sisal, thus guaranteeing their observance of privacy and security requirements and therefore the correct processing of personal data along the entire chain. **Training:** organisation and management of regular training for third parties. Training is tailored for the processes they manage on behalf of Sisal, so ensuring they know about the company processes and procedures to follow and the applicable legal requirements.

Security

For Sisal, the protection of corporate information assets and the management of ICT and security risks are objectives of primary importance.

Sisal sees **protection of its information assets** and **management of ICT and security** risks (including cyber risks) as objectives of prime importance to be pursued on a continuous improvement basis.

Cybersecurity is an enabling factor in the pursuit of business objectives. Given the increasing frequency of cyberattacks in recent years, and with the aim of continuously strengthening protection systems and ensuring security in the context of its customer services, we have defined a **cybersecurity strategy** based on the following principles:

- guaranteeing **central security governance** designed to preserve the confidentiality, integrity and availability of the company's information assets;
- promoting the development and ongoing evolution of **security technology solutions** to ensure Sisal has a sustainable advantage in the long-term and in line with its objectives and values;
- favouring the construction of an adequate **organisational model for managing information security** in line with growth objectives and promoting development of the skills needed to keep effective protection systems in place;
- guaranteeing **compliance with applicable laws, regulations and standards** that impact information security, as well as with specific contractual agreements with various stakeholders;
- promoting **innovation in the field of security** to guarantee constant alignment with new technological developments and use of new generation methods, processes and solutions;
- guaranteeing **data security, resilience and protection** in the context of services offered to consumers and clients, thereby increasing their reliability;

- spread a **culture of information security and sensitivity to cyber risks** in Sisal in order to raise the level of awareness about the behaviours involved and guidelines to follow to forestall threats;
- promoting adoption of a **risk-based approach** to choosing security measures by means of a framework built into the company's overall risk management model.

Sisal's cybersecurity strategy covers the following areas:

Security governance

Our cybersecurity strategy requires us to keep abreast of state-of-the-art security in our sector and aligned with changing risk scenarios. The Chief Information Security Officer (CISO) provides strategic vision and ensures ongoing improvement of processes to mitigate the cybersecurity risks we face. For this reason, the CISO and their organisation work in synergy with Management, with the Business Areas and Markets, HR, Internal Auditing and Risk Management functions, and with the Compliance area. The main areas involved are:

- **Strengthening the organisational structure of the Security function**: in line with the organisation's growth and the expansion of the business into international markets, Sisal has scaled up the Security function and introduced new professional roles to upgrade the management of our security capability.
- **Security certifications:** Sisal implemented and maintains an Information Security Management System that incorporates the guidelines set out in the main industry standards and regulations, including ISO27001 and WLA-SCS[35]. To further improve measures in place to guarantee the resilience of our business, in 2022 we obtained ISO22301 certification of our operational continuity management system[36]. Sisal has also obtained and maintains **ISS SGAD** certification (Information Systems Security - Sistema di Gioco di Abilità a Distanza), the gaming platform certification required by the Remote Gaming Office of the Gaming Taxation and Monopoly Central Office (Sisal Entertainment S.p.A.). The compliance of our management systems is verified by periodical audits and checks by independent third parties.
- **Security Framework:** to define security requisites, adapt them for specific processes and verify their effectiveness, Sisal has developed and maintains a framework of policy, procedures and guidelines that it keeps constantly updated. The framework has first, second and third level controls and indicators for continuous monitoring.
- **IT & Cyber Risk management:** risk assessment plays a major role in defining objectives and guidance for protection measures. To this end, Sisal has defined an ICT and Cyber Risk management model that involves assessment and monitoring of the organisation's exposure to such risks and identification and implementation of risk mitigation measures.

[35] Certification issued by the World Lottery Association in compliance with specific gaming sector and international lottery standards. The perimeter includes Sisal Lottery Italia S.p.A, Sisal Loterie Maroc and Sisal Sans.
[36] The ISO27001 certification perimeter includes Sisal Lottery Italia S.p.A., Sisal Loterie Maroc and Sisal Sans. The ISO22301 certification perimeter includes Sisal Lottery Italia S.p.A. and Sisal Entertainment S.p.A.

Cybersecurity culture

Ensuring that people across the entire organisation are adequately informed on cyber risks and ways to reduce them is of vital importance for the company's business objectives and is achieved through:

- **Security Awareness:** Sisal regularly organises awareness sessions on various communication channels and tests their efficacy by simulating attack scenarios to verify the organisation's capacity to react effectively.
- **Security Training:** Training is provided at all levels in the organisation, including contractors, and tailored to specific roles. In 2022, training sessions were held on secure source code development for teams engaged in the software development life cycle: this helps avoid the occurrence of vulnerabilities in customer applications and services.

Security enforcement

Technological developments, digitisation of services, adoption of cloud services and the evolution of cyberattack scenarios are some of the phenomena that Sisal sees as drivers to strengthen its security posture. In 2022, initiatives were completed in the following areas:

- **Prevention:** Sisal has invested in the upgrading of its security capability by implementing new generation technological solutions. Priorities here were upgrading the access control system and identity management procedures, including those with privileged access, and protection measures for the devices employed by users to carry out their tasks. Other prevention initiatives included improvements to data protection measures using encryption and anonymisation techniques and upgrading vulnerability management technologies by adopting a risk-based approach. Security testing activities are also carried out continuously, both linked to software development cycles and performed at random on critical systems, and periodical internal and external audits are conducted at least annually. Lastly, Cyber Threat Intelligence practices were further improved to prevent, as far as possible, cyberattacks or events capable of negatively affecting the Sisal brand.
- **Detection & Response:** investments in security technologies were also made to boost effectiveness in the security event and incident identification and response phases, strengthening both proactive and reactive protection measures, and there was a constant focus on gaming services. Monitoring and alarm functions signalling anomalous events or behaviours were extended to enhance the capacity to promptly identify cyberattack or fraud attempts. Certain security technology functions already in place were extended to expand the monitoring perimeter and upgrade our security event detection capability.
- **Resilience**: various test activities are carried out periodically to ensure that the operational continuity management system can effectively handle the main unavailability scenarios, also through penetration tests conducted with support from third parties.

Responsible supply chain management

For sustainability to be pursued in the medium-long term, challenges must be shared by everyone in the Sisal community, from suppliers to points of sale. We are therefore committed to **promoting our sustainability strategy along the entire chain**.

Our suppliers

Our growth and consolidation as a company were made possible by building a network of **strategic partnerships** with numerous **suppliers**, carefully selected because they have the best specialist skills available on the market and are aligned with our values and objectives: **legality, business ethics, loyalty, fairness, transparency and meritocracy**. We have more than **1,700 suppliers**[37].

[37] The number of suppliers includes those in the Italian perimeter and its foreign subsidiaries.

Types of supplies

Gaming Terminals, Gaming Materials, Logistics and Transport Services, HW Installation and Maintenance, Call Centre Services, Media, Events, Marketing, Creativity and Market Research, Voice Communication and Data Transmission Services, Hardware and Software, Gaming Platform, Consulting and Professional Services, Refurbishment Contractors, Personal and Building/Point-of-Sale Services, Food & Beverage, Sisal Television, Data Centre Services.

Our international development in recent years has led to the **internationalisation of procurement procedures** in order to obtain better contractual conditions for our foreign sites. To ensure consolidation and the continuous improvement of our procedures, our foreign procurement teams are constantly backed up by our **central Procurement function**, which supervises and supports the purchasing of products and services.

As happens for the Italian market, the **International Procurement function** oversees all **negotiating activities** with the supply chain for each of our foreign branches. These activities include scouting for new suppliers, sourcing (preparation of tender documentation, assessment of offers, and selection and contracting of suppliers), and uploading contracts to the procurement platform.

Assessment and qualification process

Under our **Quality Management System**, we apply a stringent **assessment and qualification** process to suppliers that requires them to stay aligned with the requirements of new legislation in the gaming industry and with our stakeholders' expectations.

All our suppliers are required by contract to comply with the rules and principles set out in the **Code of Ethics and Conduct**, including the **obligation to operate in line with our ethical standards** regarding employees' rights, environmental protection and workplace health and safety. We have introduced control systems for the **prevention of corruption** according to standard UNI ISO 37001:2016. Our procurement processes also take account of the characteristics that services, facilities and tools must have in order to ensure full accessibility, usability or adoption by everyone, in line with our commitment to the inclusion of people with disabilities[38].

Suppliers are assessed on the basis of their **compliance** with the provisions of contracts and orders, as well as by **monitoring** variance between the **service levels agreed** and those actually delivered and other factors such as delivery times, quality, costs and other contract specifications. These controls are used for global supplier analysis and a twice-yearly updating of the **Vendor Rating Index (VRI)**, which records suppliers' overall performance and flags areas for improvement.

[38] For more details, see our human rights and non-discrimination policy.