INTERNAL CONTROL MANUAL

FEBRUARY 2026

sonepar

Powered *by* **Difference**

TABLE OF CONTENTS:

DOCUMENTS OF REFERENCE AVAILABLE ON THE INTERNAL CONTROL SHAREPOINT:

1. Code of Conduct
2. Group Compliance Manual
3. Business Partners Code of Conduct
4. Group Approval Matrix
5. RFA process' guide
6. Financing, treasury & systems – procedures manual
7. Internal Control annual report - template
8. Annual Representation Letter – template
9. Acquisition Manual
10. Fraud, Corruption & Influence Peddling reporting template
11. HSE Group Policies
12. IT Security reference documents
13. SOD matrix
14. Mapping of Control Points vs Risks
15. Anti-corruption control plan
16. Human Rights Policy
17. Group Travel and Expenses guidelines
18. Group safety and security guidelines when traveling
19. Report of export in non Sonepar countries
20. Supply Chain transportation guidelines
21. Supply Chain Planning Playbook
22. Branch KPIs dashboard (fraud prevention)
23. Fraud Prevention cards & IC Toolkit
24. Group Chart of Accounts
25. Supply Chain Analytics - KPIs definition
26. Golden Safety Rules

Tone at the Top

We believe Internal Control is necessary for successful operations. Building a strong Internal Control environment helps to ensure compliance, secure our activities over the long term, and achieve the Group's primary objectives by managing and mitigating risks.

The Sonepar Internal Control Manual defines a robust and standardized control framework that covers an extensive range of structuring operating rules and processes.

Effectiveness of, and alignment to, these measures, throughout all entities, are expected to make Sonepar "La Référence" in the area of Internal Control and risk management and will foster profitable and sustainable growth.

Let us all share, promote and implement these common principles.

User guide

WHAT IS INTERNAL CONTROL?

Internal Control is a **process**, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the **achievement of objectives** in the following categories:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting,
- Compliance with applicable laws and regulations

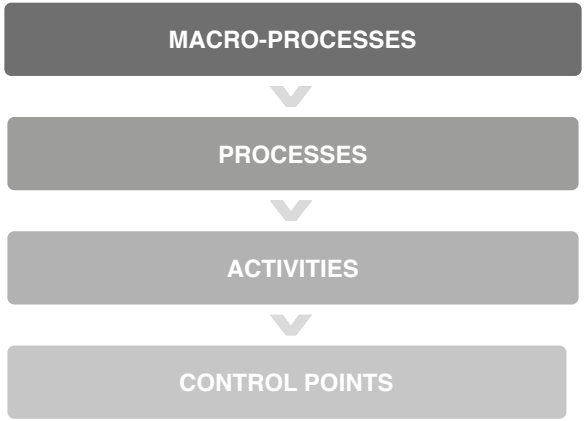
Definition from the COSO Integrated Framework (Committee of Sponsoring Organizations of the Treadway Commission)

OBJECTIVES OF THE MANUAL

This Internal Control Manual (hereafter 'Manual') is intended to support the **implementation** and **assessment** of Internal Control within Sonepar. **It defines the minimum mandatory controls representing Sonepar's standards** for operational effectiveness and efficiency. In case of Internal Control standards at local level, these should **at least incorporate the Group's standards** and more, where applicable.
The Manual supports a process geared towards developing Internal Control awareness and promotion within the entire organization.
It aims not only to ensure compliance with applicable laws and regulations, the Group Code of Conduct and Sonepar's policies and procedures, but also to protect our business and the value we create every day, aligned with best market practices.

- It reduces uncertainty surrounding our people, reputation, operations, and finances.
- It improves compliance, integrity, effectiveness, and efficiency of our processes.
- It supports decision-making with a common view of process maturity across the Group as a whole.
- It encourages **constant improvement** (dynamic process), and aims to promote Internal Control as **everyone's business**, in order to achieve our ultimate goal of becoming "**La Référence**" in our industry.

Resulting from a collaborative effort from Sonepar field experts, the Manual is structured in 8 Macro Processes (Sales & Marketing, Purchasing, Supply Chain, Merger & Acquisition, Finance, Information & Technology, Human Resources, Governance, Risk & Compliance), which describe how operations are run. These 8 Macro Processes are divided into process(es). For each process(es), one or more activities have been identified to reflect our core business. This new classification respects the following levels of hierarchy:



The Manual is intended to cover all the Group's processes and facilitate the sharing of best practices.
The objective is that all entities **fully comply with Group Standards.**

The first version of this Manual was drafted and approved by the International Finance Committee (IFC) in July 2012 and became effective early 2013. Since then, it has been regularly updated with inputs from business, functional, and control experts across the Group.

SCOPE

Internal Control applies to all processes where controls are performed. The implementation and review of controls must include all operating companies (hereafter OPCOs), holding companies, and service companies, as well as shared service centers.

TAGS

Key Controls:
In order to bring more visibility, key controls, which mitigate our most critical risks, have been underlined and defined.
Throughout all the controls, which are the Group's minimum requirements and standards, key ones were identified following a combined analysis made by various experts and members of our Internal Control function, who assess business risks with their judgments and experiences.
You will be able to identify these key controls with a key symbol beside them.

Sapin 2 Controls:
Controls that mitigate the corruption risk, in compliance with the Sapin 2 law, have been underlined. You will identify them with a symbol beside each control.

Cybersecurity Controls:
Controls that mitigate cybersecurity risk, have been selected in collaboration with the Group IT security team. You will be able to identify them with a symbol beside them.

CSR Controls:
Controls related to the Corporate Social Responsibility (in compliance with CSRD regulation) have been identified. They are tagged with a symbol beside them.

New Controls:
Controls, which have been added in this latest version of the manual are tagged with a NEW symbol beside them.

SOD MATRIX

Segregation of Duties (SOD) is a key Internal Control aspect intended to reduce the occurrence of errors and frauds, by ensuring that no employee has the ability to neither perpetrate and conceal errors, nor commit fraud in the normal course of his/her duties.

Presented in the appendix, we formalized a SOD Matrix **presenting standard toxic task combinations, which must be prevented.**
In the event that certain tasks can't be split (even in the case of temporary allocation of incompatible functions), we defined **minimum mitigating control(s)**: automatically configured in the system, preventive manual controls, or corrective manual controls - which must be implemented in order to prevent errors or fraud risks.

These expectations are mapped with the associated control points outlined in the Manual. This Matrix also includes prerequisites to be followed in order to adapt it locally.

MAPPING OF CONTROL POINTS AND RISKS

To achieve the objectives set by management and be aligned with our strategy, we have to manage the risks to which we are exposed by putting in place daily, concrete, and adequate controls.

The latest Sonepar Risk Mapping (2025) presents 84 risks to which we are exposed, split into the following 10 categories:
- Business Strategy,
- Economic & Political Environment,
- Governance, Ethics & Compliance,
- Finance,
- Operational Performance & Service Level,
- Information Technology,
- People,
- Environment & Climate,
- Social & Human Rights
- Offer.

Each control defined in this Manual covers one or more risks. They are identified below each Control Point.

The mapping between control points and main associated risks (up to four), is presented in the appendix.

REFERENCE FRAME AND SUPPORTING TOOLS

As it represents our common Sonepar language and ambition regarding Internal Control, the Manual is available to everyone in the organization. It can be found on the Sonepar Intranet MySonepar, in the section "Support Functions/ Finance/ Internal Control".

Once a year, compliance with Sonepar's standards and level of maturity is evaluated through a **self-assessment** questionnaire.
The questionnaire, while not exhaustive, is a tool to help all entities to check their compliance with key elements. This is a useful opportunity to develop awareness between operational managers and the supporting teams by sharing documentation and knowledge! Once again, **the Group's objective is 100% compliance with Group standards.**

This assessment process is performed in a GRC Group tool TRACS, enabling local process owners to assess their controls within their designated perimeter online. This information is then shared with all relevant management levels. **In the event of non-compliance with a Group standard, a corrective action plan must be created and entered in the system with a thorough follow-up.**

Within the local Internal Control function, we have created a dedicated 'Teams' group, where it is now easier and more enjoyable to interact and share our achievements, experiences, challenges, best practices, and questions. This group also provides all necessary documents.

CONTINUOUS MONITORING

In order to improve Sonepar's Control environment and facilitate the achievement of its objectives, having an emphasis on Continuous Monitoring is key.

We call Continuous Monitoring the on-going, transparent, and efficient way to detect, address and remediate risks through a set of dedicated controls (automated or not). Continuous Monitoring is a key success factor for securing business and competitiveness, while ensuring compliance.

Continuous Monitoring is the operational teams' first responsibility. They perform regular risk-mitigating controls, which are reviewed and challenged by the direct management to continuously update, complete and adjust the controls when necessary.
Local and Group 'second line of defense' teams (especially Internal Control, Risk Management, Compliance, Legal), are part of the Continuous Monitoring process, who perform regular, independent controls and reviews, challenges and monitor action plans.

These continuous controls can be performed and formalized within TRACS.

FEEDBACK

One of the main outputs of this process is a continuous improvement of our Internal Controls and operational efficiencies thanks to facilitated good practices exchanges. Please do not hesitate to communicate suggestions, concerns and questions which will be taken into consideration in subsequent updates. The local and HQ Internal Control teams are available to assist you.

Frequently Asked Questions

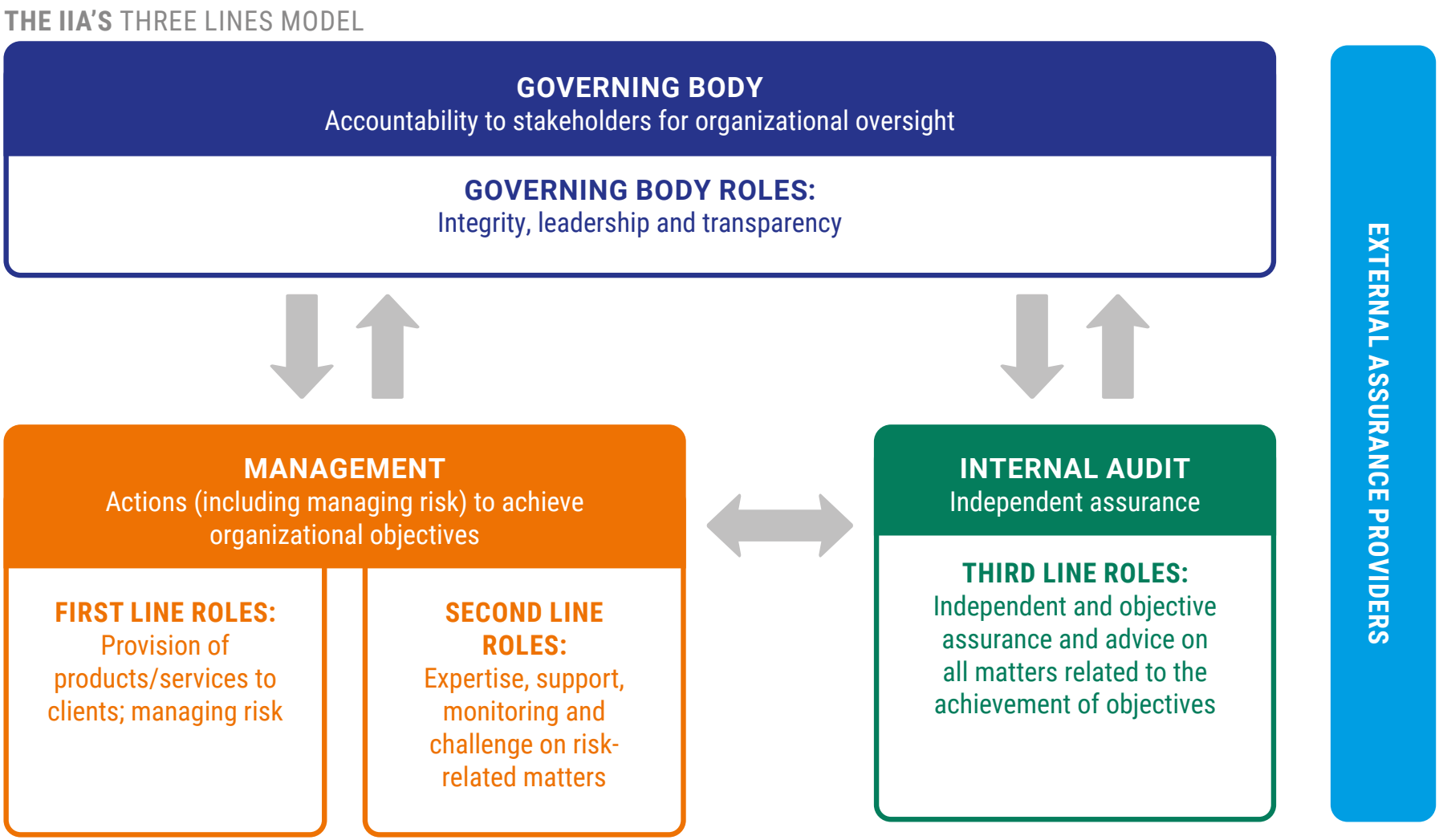
GLOBALLY

WHAT IS A RISK?

A risk is the threat that an event, action, or non-action will adversely affect an organization's ability to achieve its business objectives and execute its strategies successfully. A risk is measured in terms of consequences and likelihood.

WHAT ARE THE 3 LINES OF DEFENSE?

In July 2020, the Institute of Internal Auditors (IIA) proposed a new model of the three lines of defense:



It clearly outlines the roles and responsibilities of the governing body, executive management, and internal audit. These roles are not limited to risk management but focus on the overall governance of the organization.

Principles of the 3 lines of defense model:

Principle 1: Governance of an organization requires appropriate structures and processes that enable accountability, action, and assurance.

Principle 2: Governing body roles ensure that appropriate structures and processes are in place for effective governance.

Principle 3: Management's responsibility to achieve organizational objectives comprises both first and second-line roles. First-line roles (operational management), are most directly aligned with the delivery of products and/or services to clients of the organization. Second-line roles (Internal Control, Risk Management, Compliance, corporate functions…), assist with managing risk.

Principle 4: In its third-line role, internal audit provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management. It achieves this through the competent application of systematic and disciplined processes, expertise, and insight. It may consider assurance from other internal and external providers.

Principle 5: Internal audit's independence from management responsibilities is critical to its objectivity, authority, and credibility.

Principle 6: All roles working collectively contribute to the creation and protection of value when they are all aligned and prioritize the interests of stakeholders.

FOCUS ON SONEPAR

WHAT ARE SONEPAR'S INTERNAL CONTROL STANDARDS?

We are convinced that appropriate controls secure and strengthen operations. For this purpose, we have designed minimum, mandatory controls for our operations described in this Manual, and **we expect all Sonepar entities worldwide to be 100% compliant with these standards.**

WHAT ARE SONEPAR'S INTERNAL CONTROL REPORTING EXPECTATIONS?

Every year, the following documents must be submitted to the Group:

1. Internal Control self-assessment completed by each OPCO, holding company, service company via TRACS**.**
2. Annual Representation Letter (due by February 15 of each year), signed by each country's President or executive management and CFO.
3. Internal Control Annual Report from Country CFO to Group CFO (standard template; due by January 31st of each year), including a description of the past year's main achievements regarding Internal Control, a synthesis of Internal Control assessment results, a summary of frauds occured in the year, the Internal Audit engagements results, and a description of the new year's Internal Control roadmap (incl. Finance processes improvements).
4. Quarterly Fraud, Corruption, and Influence Peddling reported in TRACS (due by April 15th for Q1, July 1st for Q2, October 15th for Q3, and January 15th of the following year for Q4), including any corrective and preventive actions undertaken.

WHAT DOES SONEPAR MEAN BY COMPLIANCE, FRAUD, CORRUPTION, AND INFLUENCE PEDDLING?

- **Compliance** means conforming to an applicable law or regulation, the Sonepar Code of Conduct or other internal rule, policy or standard, and acting with integrity, in accordance with Sonepar values.

- **Fraud** is any illegal act characterized by deceit, concealment, or violation of trust.
  Fraud includes Corruption (i.e. conflicts of interest, bribery, as further defined below), Asset misappropriation (i.e. cash theft, illegal diversions of assets), and Financial Statement fraud (i.e. asset overstatement, liability understatement).

In practice, it can take many forms such as:

- Fraudulent financial reporting, including distorted records, falsified transactions, or misused accounting principles resulting in intentionally misleading financial information
- Misuse of funds (false invoices, manipulation of checks, falsification of bank details)
- External or Internal thefts of Sonepar's assets (supplies, hardware, data)
- Falsification of receipts for expense reporting (claims for fictitious expenses, undeclared absences)
- Misrepresentation of a claim to a third party (supplier, insurance company)
- Intentional inaccuracies in inventory counting
- Forgery and counterfeits

Sonepar may also be exposed to external fraud attempts, such as:

- Fake CEO bank transfer instructions
- Fake bank accounts or reference numbers
- Illegal acts by third parties against Sonepar's interests

► **Corruption** includes offering, promising, giving, soliciting or accepting an undue advantage, whether financial or non-financial, directly or indirectly, to encourage or reward a person to secure business, influence the award of a contract or a public bid, or obtain a favorable decision.

Corruption generally involves at least two parties:

- The party who uses its power or influence in exchange for an undue advantage; and
- The party who offers or provides this undue advantage.

A person who facilitates an act of corruption is an accomplice, and one who benefits from this act by receiving the undue advantage is a receiver. They are personally liable for these actions.

► **Influence Peddling** is the unlawful use of one's position or influence on someone's behalf in exchange for money or favors.

Corruption is deemed to exist even if:

- The person who offers the undue advantage acts through a third party
- The person who receives the undue advantage is not its end-beneficiary
- The fraudulent action and the granting of the undue advantage do not take place simultaneously (the undue advantage may be granted in advance or at a later date)
- The undue advantage is in a non-monetary form
- The beneficiary is a public-sector employee or a private-sector employee
- Corruption and influence peddling are illegal in virtually every country and are strictly prohibited by the Group Code of Conduct.

WHO SHOULD COMPLETE THE INTERNAL CONTROL ASSESSMENT?

Controls are performed by everyone in the organization, so answers should – whenever possible – come from the people in charge – the Business Process Owners (BPOs) – and those who are most knowledgeable about the key processes that are covered. Controllers/finance teams can be facilitators but cannot answer for or in lieu of operating managers.

HOW TO COMPLETE THE ASSESSMENT?

- Organize the Assessment completion. In planning your rollout, start with the OPCOs where you feel the process will take the longest amount of time to be implemented. Also, place the OPCOs where you feel risks are higher at the top of your priorities list.
- Discuss/check each questionnaire with the OPCO team:
  - An 'Effective' assessment must be supported with pertinent documents, (procedures, reports, screen prints…).
  - A 'Non-effective' or 'Partially effective' assessment must result in action plans, (including the designation of the person in charge and the timing for the implementation thereof).
  - A 'N/A' means the control does not apply to the entity because the process is different or is performed at a different level, (e.g. a shared service center). In this case, an explanation is required.
  - A 'Management accepts the risk – Non effective' assessment requires a thorough explanation.
- It is better to have a 'Non-effective' or 'Partially effective' assessment with an action plan than an 'Effective' answer that will eventually prove to be ineffective when audited and tested!
- Gather all documentation in a file to support the controls and tests' effectiveness. This file must be made available to you and to any person likely to use it, (President, CFO, Internal Audit, OPCO Managers) or can be uploaded in TRACS.
- Prepare a summary of the self-assessment for your country/zone for discussion with your President and with the Group.
- Prioritize, track, and follow action plans resulting from this review; each action plan must have a set deadline and a project owner.

HOW TO MONITOR ACTION PLANS?

It is essential in our continuous involvement to manage our control environment maturity level, to ensure that all planned actions to mitigate risks are effectively and efficiently implemented. In TRACS, this monitoring has been facilitated with an owner and a reviewer, who all have to be involved in the process in order to provide an appropriate answer to the identified deficiency with a coherent deadline. Every year, it is under the Internal Control function's responsibility to ensure the continuous monitoring and follow-up of opened action plans, jointly with their respective owners.

Structure
of the Internal Control Manual

8 MACRO-PROCESSES

OPERATIONAL
MACRO-PROCESS

- SALES & MARKETING (10)
- PURCHASING (20)
- SUPPLY CHAIN (30)
- MERGER & ACQUISITION (40)

SUPPORT
MACRO-PROCESSES

- FINANCE & ACCOUNTING (50)
- INFORMATION & TECHNOLOGY (60)
- HUMAN RESOURCES (70)
- GOVERNANCE RISK COMPLIANCE (80)

DETAILED MACRO-PROCESSES:

SALES & MARKETING

Determine and analyze sales strategy
- Determine and analyze sales strategy

Manage negotiation of commercial terms, pricing and conditions
- Open and maintain customer account
- Manage the quotation process
- Ensure contractual relations are properly authorized and compliant with Group policy
- Manage Customer's terms

Manage credit risk
- Define, maintain and enforce credit policy
- Optimize collection and dunning process

Define the offer - Marketing sales
- Determine marketing and advertising program (incl. customers / markets / product segmentation)
- Manage customer wants and satisfaction

Manage merchandising and promotion
- Train Sales Staff
- Coordinate vendors' incentives and loyalty programs
- Follow liquidation sales

Perform billing
- Manage sales orders
- Ensure invoicing is complete and accurate following Group and local policies
- Follow disputes with customers
- Ensure credit notes are validated and properly documented
- Ensure customers' returns and claims are processed

Monitor sales
- Monitor Sales
- Follow CRM

Monitor user access
- Monitor user access

PURCHASING

Manage supplier and product data
- Manage products database
- Ensure prices are correct
- Assess and Create Suppliers
- Manage tender and selection process
- Select a supplier

Manage purchase order
- Validate purchasing price with the supplier and issue the Purchase Order
- Manage open PO

Follow vendors relationship and negotiation
- Ensure rebates programs are reviewed
- Follow vendor's obligations and incentives
- Evaluate and monitor suppliers
- Monitor SPA

Monitor user access
- Monitor user access

SUPPLY CHAIN

Planning
- Define inventory strategy
- Manage orders
- Analyze and optimize stock level

Warehousing
- Manage reception of goods
- Perform inventory physical counts
- Monitor stock adjustments
- Manage goods' returns
- Manage the warehouse
- Prepare customer order

Transport
- Manage transport activity
- Manage shipment
- Ensure customer's delivery

Monitor logistic activities
- Follow supply chain analytics
- Monitor user access

MERGER & ACQUISITION

Maintain an acquisition strategy and procedures
- Maintain market watch and strategy
- Maintain procedure awareness
- Ensure legal confidentiality

Identify target and exploratory phase
- Assess culture fit
- Assess target financials and risks

Prepare documentation for the investment committee
- Prepare business case
- Prepare acquisition sheet
- Prepare the due diligence team

Conduct due diligence on the target
- Challenge the information provided during the due diligence
- Review financial, tax, operational, legal, compliance, IT and HR aspects / status of the target
- Anticipate integration steps

Finalize legal duties and communicate about the deal
- Finalize legal duties
- Communicate the deal

Follow the integration of the acquisition within the Group
- Follow the integration of the acquisition

FINANCE & ACCOUNTING

Prepare and approve budget
- Prepare and approve budget and forecasts
- Manage investments

Manage accounting activities
- Process accounts receivable
- Process accounts payable
- Control fixed assets
- Review leases
- Establish accruals, provisions and off-balance sheet commitments process
- Close the books
- Manage bank reconciliations
- Manage SPA accounting process

Prepare and approve reporting of activity
- Prepare and approve reporting
- Perform reviews of specific accounts

Manage financing activities
- Implement local debt agreement
- Manage bank relationships and bank accounts
- Control bank fees
- Identify and define foreign exchange exposure
- Manage foreign exchange hedging
- Manage interest rate hedging
- Manage cash investments
- Manage factoring activity
- Manage financing limits
- Anticipate cash flows
- Manage payment means and treasury

Manage tax
- Manage tax activities
- Manage tax risk

Monitor shared service center
- Monitor shared service center

Manage travel expenses
- Define and maintain a travel policy
- Manage and monitor corporate credit cards
- Monitor the travel expenses reimbursement process

Monitor user access
- Monitor user access

INFORMATION & TECHNOLOGY

Plan and organize
- Define a strategic IT plan
- Ensure availability of IT resources
- Manage physical security
- Manage project

Build, acquire and implement
- Manage changes
- Manage the datalake

Deliver service and support
- Ensure continuity of systems
- Perform backup
- Ensure integrity of IT and system security
- Manage user access / Monitor super-user profile
- Control assets and applications inventory

HUMAN RESOURCES

Manage people (planning, recruitment, termination)

- Hire new employees and manage terminations
- Follow and analyze HR KPIs

Manage people's performance and development

- Evaluate employees
- Develop succession and career plans
- Develop and train employees
- Maintain objectives & strategic alignment

Ensure compliance with labor regulations

- Ensure compliance with labor regulations

Manage payroll

- Determine and approve wage plan
- Review payroll processing and other payments to management and employees (excl T&E)
- Ensure accuracy of payroll journal entries

Monitor HR activities

- Monitor user access
- Follow satisfaction survey
- Ensure data quality

GOVERNANCE RISK & COMPLIANCE

Ensure compliance with corporate standards

- Develop corporate governance
- Prevent and report fraud and abuse

Ensure legal and regulatory compliance

- Manage legal and regulatory compliance
- Manage the offering and receiving of gifts and gratuities
- Manage data privacy risk

Ensure business continuity

- Prepare a business continuity plan and manage employees training and awareness

Manage security and safety of people and assets

- Manage HSE and insurable risks
- Respect human rights

Enhance general control environment

- Maintain clear organizational structure
- Monitor Internal Control
- Manage compliance with internal audit standards
- Manage compliance with external audit standards
- Ensure compliance with company code of conduct
- Pilot board management
- Implement / maintain a whistleblowing process
- Prevent and manage corruption

Manage environmental social and governance requirements

- Manage environmental social and governance requirements

Ensure appropriate communication

- Manage crisis (in case of reputational risk for the Group)
- Manage corporate communications to journalists, radio & TV
- Establish communications plan
- Manage local communication with significant Group impact
- Publicly communicate financial information
- Create web sites / social media accounts / intranets
- Manage marketing communication
- Manage right to publish

Sales & Marketing

PROCESS:

DETERMINE AND ANALYZE SALES STRATEGY

ACTIVITIES

Determine and analyze sales strategy

PC-10-10-010-005

[Risk(s): Customer satisfaction; Dependency; Business model]

- A formal sales policy is established and validated by local management and compliance, and is periodically reviewed to ensure alignment with regulatory requirements.
- The policy clearly defines locally applicable rules governing sales activities and customer relationships, incorporates guidelines on pricing approvals, credit risk management, and anti-corruption measures.
- The policy is documented, communicated, and accessible to all sales associates.

PC-10-10-010-010

[Risk(s): Performance gap; Customer satisfaction]

- The operating company's strategic vision is deployed by each division and branch and translated into measurable sales objectives through a structured five-year plan.
- This plan ensures alignment between corporate strategy and operational execution and defines targets, timelines, and responsibilities to drive consistent performance and long-term growth.

PC-10-10-010-030

[Risk(s): Performance gap; Budget & planning; Performance measurement]

- Sales objectives are reviewed and updated by management on a monthly basis to ensure alignment with market conditions and strategic priorities.
- Objectives are assigned to both inside, outside sales associates and all sales managers based on a thorough analysis of prior-year performance and potential sales opportunities.
- Sales objectives incorporate customer segmentation and profitability analysis to ensure focus on high-value opportunities.
- A comprehensive yearly assessment is conducted by management to compare actual results against the strategic plan, identify variances, and implement corrective actions to drive continuous improvement.

PROCESS:

MANAGE NEGOTIATION OF COMMERCIAL TERMS, PRICING AND CONDITIONS

ACTIVITIES

Open and maintain customer account

PC-10-15-010-020

[Risk(s): Product/Service pricing; Corruption]

- A pricing matrix is maintained in cooperation between Marketing, Purchasing and Sales departments in order to communicate appropriate commercial offer(s) to the customer. Updates and permanent overrides of the pricing matrix are restricted, approved, documented and monitored.
- The access to pricing matrix is secured and restricted.
- The pricing matrix is reviewed and validated by Pricing department or appropriate management. A specific complete monthly review of updates and overrides is performed through the IT system and analyzed by management.
- Customer price classes are pre-defined and customers are monitored for appropriate categories.

PC-10-15-010-030

[Risk(s): Default; Third-party non-compliance; Corruption]

- There is a formalized procedure for customer account creation.
- Sales Associates are responsible for the completion of the application (customer file) to open a new account.
- The customer's information and reliability are verified through one of the following methods: online automatic authentication, an on-site visit, or a phone call to the customer's reception desk. All personal customer

and contact information must be handled in compliance with local legal requirements (e.g., GDPR).

- ► To prevent account duplication, a customer account may only be created if no existing account is already registered at the OPCO level. Exceptions to this rule are strictly limited, require approval from both Sales and Credit Management, and must be properly documented.
- ► The Sales Manager and Credit Manager (or the Finance Director, if a Credit Manager is unavailable) are responsible for approving business rules and managing exceptions and changes related to credit limits and terms.

PC-10-15-010-040

[Risk(s): Third-party non-compliance; Corruption; Default]

- ► Validation of customer file is described in a formalized procedure, which includes a review of required documentation to ensure the accuracy and completeness of customer information:
  - contract;
  - customer segmentation;
  - rebates;
  - initial terms of payment that do not exceed the standard terms defined by the organization and that comply with local legal regulations;
  - delivery and invoice addresses;
  - invoice and payment terms;
  - conditions for customer returns;
  - review of potential duplicate customer accounts.
- ► The individual who keys the customer data in the system is different from the individual who approves them.
- ► Later changes to the initial terms and conditions are subject to the same prerequisites and management approval as the initial request.
- ► Documentation is maintained and recorded in the customer file.
- ► Changes to the Customer Master File are reviewed on a monthly basis by an independent individual who does not have access to modify the customer database.

ACTIVITIES

Manage the quotation process

PC-10-15-020-010

[Risk(s): Performance gap; Customer satisfaction; Corruption]

- ► Quotations and price requests by customers are managed by the Sales teams through a defined operative procedure. It includes the following aspects:
  - The inside sales teams manage customers quotations in line with the defined instructions from local management;
  - Quotations and estimates sent to customers are reviewed and validated by management when exceeding a predefined threshold;
  - Price quotations given to customers on significant projects with low margins are thoroughly reviewed;
  - Unusual (foreign customer, new contact from existing customer, customer from another Branch, customer ordering multiple times within a short period etc.) or especially high quotations are controlled and validated through a defined escalation process;
  - Quotations for unusual products (e.g. TV, washing machine, computer…) are reviewed and validated through a defined escalation process;
  - Management regularly reviews KPIs to assess the level of service and conversion rate.

ACTIVITIES

Ensure contractual relations are properly authorized and compliant with Group policy

PC-10-15-030-005

[Risk(s): Third-party non-compliance; Corruption; Value chain workers rights]

- ► Each customer is assessed in accordance with the business partner procedure implemented locally, such procedure being in line with the Compliance Manual.
- ► This assessment is based on a risk scoring with criteria that are formally defined. Financial conditions, respect of Human Rights and corruption risk exposure are evaluated. Depending on the results of the risk assessment, a due diligence is performed on the customer.

PC-10-15-030-010

[Risk(s): Business non-compliance]

- Contracts (including General Terms of Sales) and written conditions for each customer (at least for stock item, including inter alia: discounts, volume, year- end rebate, pricing matrix) are reviewed by the legal department in accordance with internal policies and procedures involving the appropriate internal stakeholders.
- Contracts are approved in compliance with the Group and local Approval Matrices.
- Afterwards, contracts are properly executed and archived.

PC-10-15-030-080

[Risk(s): Corruption; Third-party non-compliance; Value chain workers rights]

- Intermediaries, such as business providers and agents, as well as joint venture partners are subject to due diligence in accordance with the Group "Dealing with Business Partners" policy, included in the Compliance Policy 308 of the Compliance Manual and in regards to the respect of Human Rights. This procedure is strictly followed for submitting, assessing and approving Intermediaries.
- No intermediary or joint-venture partner may be retained without the formal assessment, due diligence and approval provided in the Group Procedure.
- For each active or new intermediary or joint-venture partner account, as a minimum the mandatory questionnaire is completed and a search for records is undertaken on an external database.
- The contracts with intermediaries and joint-venture partners are reviewed and approved by legal department as part of the due diligence process and in compliance with Sonepar policies and procedures.
- "High risk" intermediaries are approved in writing by the relevant Sonepar Executive Group (SEG) functional member or the relevant Regional President.
- Other intermediaries are approved in writing by the Country top manager.
- Intermediaries' services and costs are reviewed and controlled every month by someone independent from sales and marketing activities.
- Remunerations granted to sales intermediaries are subject to a contract and an activity report. They are booked in a specific account, justified (with reality of the service given) and controlled (compliance with terms negotiated).

ACTIVITIES

Manage Customer's terms

PC-10-15-050-010

[Risk(s): Business non-compliance; Corruption]

- For key accounts, contractual negotiated aspects (year end bonuses, service level etc) are annually monitored and followed by management.

PC-10-15-050-020

[Risk(s): Anti-competitive practice; Performance gap; Corruption]

- There is a specific procedure related to customer year-end bonuses, including agreement, monitoring and payment processes.
- Customers' year-end bonuses are monitored by someone independent from direct management and sales activity. Year end rebates must not be settled by personal gifts or benefits to customers (for example, products...). They are controlled to ensure they comply with the terms and conditions agreed in the contract.

PROCESS:

MANAGE CREDIT RISK

ACTIVITIES

Define, maintain and enforce credit policy

PC-10-25-010-010

[Risk(s): Default; Performance gap]

- Credit policy is established at company level. It includes at least:
  - procedure of opening and maintenance of customer account (documents, thresholds, criteria, approval process);
  - definition of payment terms and credit limits rules;
  - debt collection process;
  - bad and doubtful debts monitoring procedure (including review, approval authority, documentation requirement, and expected write off timeline);
- It is reviewed annually by the Credit Manager.

PC-10-25-010-040

[Risk(s): Default; Performance gap]

- Below a certain credit scoring and in the absence of any credit insurance, a deposit, collateral, bond or other form of tangible or personal guarantee is given by the customer or by a trustworthy third party (bank or end-customer).

PC-10-25-010-050

[Risk(s): Default; Performance gap]

- Customer's P&L and Balance Sheet are analyzed regularly, at least annually for strategic customers in order to follow up credit exposure and to manage credit risk.
- IT controls are established to prevent override of approved credit limits.
- Customer accounts exceeding their approved credit limit are put on hold in the system.
- Customer accounts exceeding their aging terms are addressed with the contact and risk escalation procedures in place to ensure every instance is dealt with appropriately (and if necessary put on hold in the system).
- New customers are automatically blocked in the system after their first invoice not paid.
- Rules for releasing/unblocking customers on hold are defined and followed, according to segregation of duties.
- Credit limits holds (placement and removal) are reviewed regularly according to the amount of credit given (threshold are predefined in the local policy validated by management). They are communicated to the sales team.
- Customer accounts close to credit limit are reviewed in a timely manner to prevent sales blockage & manage credit risk exposure.

PC-10-25-010-110

[Risk(s): Default; Performance gap]

- A measurement of the respective amount of account receivable insured, not insured and refused by the insurance company is reviewed by management.
- Management reviews measurement of account receivable guaranteed by third parties.

PC-10-25-010-120

[Risk(s): Default; Performance gap; Corruption]

- Cash on delivery (COD) customers (defined as customers required to pay at the time of delivery, regardless of payment method) are formally identified in the system and monitored by the Credit Manager at least monthly. The review must include, not limited to, high transaction amounts, reasons for COD status, recurring issues, and the existence of other blocked or high risk accounts linked to the same customer. Follow up actions must be documented and escalated when necessary.

ACTIVITIES

Optimize collection and dunning process

PC-10-25-020-010

[Risk(s): Default; Performance gap; Corruption]

- Aging balance and trend analysis are produced each month at company and branch level from the IT system following the Group template, reconciled with General Ledger and reviewed by Finance director and systematically available and communicated to:
  - sales team;
  - branch manager;
  - credit manager;
  - regional manager;
  - company's general manage;
  - country's general manager.

PC-10-25-020-030

[Risk(s): Default; Performance gap]

- Regarding credit risk, an aging analysis is performed at least monthly for insured customers to make sure collection procedures requested by the credit insurer are properly followed in accordance with the written procedure for insured customers. The implementation or removal of credit insurance lines requires the Group CFO prior approval.

PC-10-25-020-040

[Risk(s): Default; Performance gap]

- ► Bad debt collection and dunning activities are reviewed by the credit department following a procedure that specifies:
  - required documentation for dunning activities (customer address, email, phone number);
  - standards time intervals to initiate contact and to take subsequent appropriate actions depending on past due status;
  - supervisory review of customer collection file;
  - the processes and approvals required for payment discrepancies, short payment and disputes.
- ► The IT system can generate automatic reminders based on preconfigured dunning parameters.

PC-10-25-020-070

[Risk(s): Default; Performance measurement]

- ► Sales management reviews indicators related to credit management.
- ► Main ratios are:
  - DSO;
  - bad debt expenses;
  - evolution of number of doubtful customer accounts followed and solved by Credit Department.

PROCESS:

DEFINE THE OFFER - MARKETING SALES

ACTIVITIES

Determine marketing and advertising program (incl. customers / markets / product segmentation)

PC-10-35-010-010

[Risk(s): Performance gap; Customer satisfaction]

- ► A program for marketing and advertising activities is set up, documented and validated by management.
- ► At a minimum, this program:
  - is co-designed with the Sales and Purchasing departments, to identify and act on opportunities to attract and retain customers;
  - is determined in accordance with the marketing plan of the parent company / parent country where applicable;
  - takes into account locally available digital transformation initiatives, such as e-commerce platforms, marketing automation, CRM systems, mobile apps, S2S/EDI, and digital customer touchpoints;
  - monitors competitor's marketing initiatives and their impact on market shares;
  - leverages customer data and analytics to inform marketing strategies and measure program effectiveness.

ACTIVITIES

Manage customer wants and satisfaction

PC-10-35-020-010

[Risk(s): Customer satisfaction]

- ► Customers' surveys are performed at least twice a year in order to capture customer insights and measure satisfaction.
- ► Survey results are presented and discussed at top management level locally.

PROCESS:

MANAGE MERCHANDISING AND PROMOTION

ACTIVITIES

Train Sales Staff

PC-10-45-020-010

[Risk(s): Skills and knowledge capital; Customer satisfaction; Performance gap]

- ► Trainings or communications are organised, as frequently as needed, by the Marketing and Purchasing departments to familiarise Sales teams with products, marketing activities, vendor incentives and loyalty programs.
- ► Sales department provides inside and counter sales teams with all the necessary information to recommend products to customers (technical or commercial information, pricing lists, pricing matrix, products availability, last quotations or sales).

ACTIVITIES

Coordinate vendors' incentives and loyalty programs

PC-10-45-040-010

[Risk(s): Corruption; Business non-compliance; Customer satisfaction]

- ► Vendors' incentives, rewards and loyalty programs are established based on sales objectives and approved by management according to contractual conditions with vendors. They are documented, validated by legal and approved by customers as part of the business terms and conditions.

ACTIVITIES

Follow liquidation sales

PC-10-45-060-010

[Risk(s): Corruption; Misappropriation of assets; Performance gap]

- ► There is a validated process on liquidation sales (e.g. obsolete stock items or with low rotation) : product category, period, price… This processes designates owner(s) for the management and execution of the liquidation sales. Liquidation sales must be specifically identified in IT systems and properly followed in stock.

PROCESS:

PERFORM BILLING

ACTIVITIES

Manage sales orders

PC-10-60-010-010

[Risk(s): Performance gap; Business non-compliance]

- ► All customer orders are documented and reviewed by the Sales Department to ensure:
  - arithmetic accuracy;
  - margin and profitability;
  - compliance with contract terms and pricing. (Orders that do not meet requirements must be rejected except sales orders entered by sales associates with special permission to override prices);
  - all mandatory information is provided by customer (prices, delivery address...);
  - recent changes in customer's contact person are challenged through a proper verification process, such as a phone call to the company, to ensure the reliability of the contact placing the order;
  - unusual circumstances, such as the sale of sensitive or high-value materials, customers from another branch, foreign customers, multiple orders in close succession, unusual delivery sites, etc. are challenged;
  - any potential ethical or compliance issues are identified;
  - foreign customers are checked to determine whether export control regulations apply to the particular transaction and, if applicable, due diligence is conducted to ensure the foreign customer is not a blocked individual an OFAC Specially Designated National (SDN), or is not owned, directly or indirectly, 50% or more by one or more such blocked persons, as described in the Compliance Manual.
- ► Access to approve price quotes in system is restricted to authorized associates.

PC-10-60-010-040

[Risk(s): Customer satisfaction; Performance gap; Corruption]

► A review, analysis and reconciliation of open-orders (undelivered orders, goods shipped not invoiced) are performed on a monthly basis. This reconciliation is approved by a supervisor, and the resolution of open items is documented and maintained on file.

ACTIVITIES

Ensure invoicing is complete and accurate following Group and local policies

PC-10-60-030-020

[Risk(s): Accounting information; Corruption]

► A formalized procedure is established and strictly applied, detailing invoice issuance rules, revenue recognition criteria and related controls outlined in the relevant control point.
► Any exceptions (e.g., consignment, bill-and-hold, or agent transactions) must be documented and comply with Group policy and IFRS 15 requirements.
► For stock sales' revenue is recognized upon transfer of control (ownership and responsibility). Invoicing must be performed as defined in the sales contract.
► Controls are performed to ensure revenue is recognized in accordance with IFRS 15 and Group policy (most of the time transfer of control means shipment, attention must be paid to incoterms).
► For direct sales, revenue is recognized upon confirmation of shipment or delivery by the supplier, aligned with the transfer of control. Controls are performed to ensure all conditions are met. Invoicing must occur in the same accounting period.

Direct Sales refer to selling products that are delivered directly from Sonepar's supplier to Sonepar's customer without transiting through Sonepar premises (CDC, Hub, Branch…). They require specific attention as goods can only be invoiced to the customer once Sonepar has received the delivery confirmation.

PC-10-60-030-040

[Risk(s): Performance gap; Accounting information]

► Invoicing of additional services (as loan of equipment to customers or specific transport costs for deliveries) is monitored by Sales Department according to contractual conditions.

PC-10-60-030-050

[Risk(s): Business non-compliance; Corruption]

► Shipping documents are matched, either manually or electronically, with approved customer Purchase Orders and differences are followed-up by authorized persons prior to generating the related sales invoices.
► After print-out, no modification can be done.

PC-10-60-030-060

[Risk(s): Accounting information; Business non-compliance]

► Sales system prevents users from issuing invoices after an accounting closing is performed.

PC-10-60-030-070

[Risk(s): Business non-compliance]

► Invoices must include the following information to ensure compliance with business and legal requirements:
- legal entity responsible for invoicing;
- customer billing address;
- delivery address;
- reference to the sales orders;
- products quantity, unit prices;
- currency of the invoice;
- freight charges, INCOTERM;
- applicable VAT and sales tax;
- payment terms;
- a unique sequence number.

► Invoicing must be performed without possible change, and archived either in the invoices file or customer file.
► The use of manual invoices is prohibited.

ACTIVITIES

Follow disputes with customers

PC-10-60-040-010

[Risk(s): Performance gap]

- ► All pending commercial disputes are followed by Sales Department and reviewed by Legal Department if need be.

ACTIVITIES

Ensure credit notes are validated and properly documented

PC-10-60-050-010

[Risk(s): Business non-compliance; Corruption]

- ► A formalized procedure is in place covering all types of credit notes, including manual credit notes and those automatically generated by the system, and defines the associated governance such as granting criteria, authorization workflow, documentation requirements, and monitoring processes.
- ► All credit notes must be justified, supported with appropriate documentation, and approved by management prior to issuance.
- ► The use of gifts or any other benefits to customers as a substitute for credit notes is strictly prohibited.
- ► A monthly credit notes report is generated from the accounting system, reconciled to the general ledger, and analyzed to identify trends and abnormal patterns. The analysis includes:
  - reason for issuance (e.g., customer error, sales entry error, logistics or warehouse processing errors in product or quantity, transport damage, transport damage, products no longer needed by customer);
  - issuance rate at OPCO level (credit notes/turnover);
  - issuance rate by branch (branch credit notes/branch turnover);
  - issuance rate by customer (customer credit notes / customer turnover).

ACTIVITIES

Ensure customers' returns and claims are processed

PC-10-60-060-010

[Risk(s): Performance gap; Business non-compliance]

- ► There is a procedure which clearly defines how to handle returns of products with respect to the causes for returns: defective product returns or commercial returns.
- ► Return costs (transport) are invoiced to customers according to commercial conditions.

PROCESS:

MONITOR SALES

ACTIVITIES

Monitor Sales

PC-10-65-010-010

[Risk(s): Performance measurement; Dependency; Corruption]

- ► There is a monthly analysis of customer sales by:
  - comparing actual sales to initial monthly objectives;
  - reviewing the numbers of new accounts and active customers contributing to each Sales portfolio and sales divisions;
  - analyzing sales by customer, customer segment, sales division and by product group;
  - analyzing e-commerce sales (e-business, mobile, S2S);
  - reviewing promotional operations, new products;
  - reviewing dependency to main customers;
  - ensuring that collusion is prevented;
  - analyzing profitability (with actions taken as deemed appropriate);
  - monitoring margin levels by customer, customer segment, sales division and by product group.

PC-10-65-010-020

[Risk(s): Performance measurement; Corruption]

- Margins by customer are analyzed by management.
- Transactions with excessively low or high margins are followed up daily and reported to Sales teams and management.
- Any transactions showing significant deviations from the standard terms and conditions defined by local management are blocked by the IT system, especially in case of negative margin.

PC-10-65-010-100

[Risk(s): Performance gap; Business non-compliance]

- There is a formalized and documented procedure for defining commissions for sales associates.
- The calculation of such commissions are based on a contract or agreement or a company commission plan.
- The process defines who can modify and approve changes to the commission calculation grid and must ensure segregation of duties between the different tasks in the process (e.g. target definition, validation and calculation) in the process.

PC-10-65-010-110

[Risk(s): Performance gap]

- Sales Management reviews and validates the eligibility of the salesperson and the commission amount to be paid.
- Commission adjustments and exceptions are authorized and approved by the appropriate level of Management.
- Commission payments are validated and authorized by Finance or HR.

NEW PC-10-65-010-120

[Risk(s): Business non-compliance; Authority/limit]

- There is a formalized procedure specifying the rules for sales to internal staff. It defines among others the minimum sales price, the maximum volume (in value) allowed per year, the type of products authorized, the permitted payment terms (immediate payment) and the respect of local tax requirements.
- There is at least a yearly monitoring of these transactions by associate (performed by Finance or HR).

ACTIVITIES

Follow CRM

PC-10-65-030-010

[Risk(s): Performance gap; Customer satisfaction]

- A CRM tool is implemented to streamline sales, customer service, contact centers and marketing processes. For OPCO not yet equipped, implementation must be coordinated with Spark team.
- Accounts and business contacts (individuals) are recorded and maintained in the tool, to prevent duplication and ensure data accuracy.
- Customer contact consent and communication preferences are managed in accordance with local data protection regulations, such as the General Data Protection Regulation (GDPR).

NEW PC-10-65-030-020

[Risk(s): Performance gap; Customer satisfaction]

- Sales business opportunities are systematically monitored and included in forecasting activities, with dedicated review sessions led by the sales managers, at least on a monthly basis. These reviews ensure visibility on pipeline evolution, highlight potential risks or gaps, and support informed decision-making for future sales actions.

PC-10-65-030-030

[Risk(s): Performance gap; Customer satisfaction]

- Sales activities are systematically tracked and monitored, with at least monthly performance reviews conducted by the sales managers.
- Customer and prospect visit planning are also reviewed and validated by management on a monthly basis to ensure alignment with commercial priorities.
- In addition, weekly follow-up meetings are organized by local management with field teams to assess progress, address challenges, and coordinate upcoming actions.

PROCESS:

MONITOR USER ACCESS

ACTIVITIES

Monitor user access

PC-10-80-010-010

[Risk(s): Access; Authority/limit]

- ► Managers are in charge of ensuring that proper segregation of duties is in place.
- ► Annual access reviews are performed (applications, networks…).
- ► User access to sensitive sales transactions (pricing matrix, invoicing, credit notes issuance…) are secured and monitored.

PC-10-80-010-020

[Risk(s): Performance gap; Access]

- ► A policy is established specifying which associates role have access to gross profit and cost information and for which business area.
- ► Access to gross profit and cost information is not granted to certain associates such as counter associates.
- ► Access reviews are performed at least annually.

Purchasing

PROCESS:

MANAGE SUPPLIER AND PRODUCT DATA

ACTIVITIES

Manage products database

PC-20-10-010-010

[Risk(s): Performance gap; Supply/Sourcing]

- There is a procedure for creating an article in the database and deciding whether to stock it or not. This procedure also outlines the determination of purchase needs, including methods for estimating quantities, an optimal order quantity calculation and minimal inventory levels.
- The full product lifecycle (for stock or non-stock article) from creation, through maintenance, until end of life, is monitored in the database.
- For every product a unique identification is defined (a supplier, a product ID and an internal product owner) for monitoring purposes and controls are implemented to ensure that the master product file is reliable.

ACTIVITIES

Ensure prices are correct

PC-20-10-030-010

[Risk(s): Performance gap; Corruption]

- Prices lists and conditions received from suppliers are systematically examined and evaluated by the procurement department. The purchasing IT module also includes some controls to limit the procurement risks, especially concerning products with an actual price not compliant with the negotiated price / approval matrix. Price calculations for sell-in and sell-out (incl. packaging format) are also governed.
- The purchase price and the rebate structure are confidential and secured.

ACTIVITIES

Assess and Create Suppliers

PC-20-10-040-005

[Risk(s): Third-party non-compliance; Corruption; Value chain workers rights]

- Each new supplier is assessed in accordance with the business partner procedure implemented locally, such procedure being in line with the Compliance Policy 308 of the Compliance Manual.This assessment is based on a risk scoring with criteria that are formally defined. Quality, financial conditions, respect of Human Rights and corruption risk exposure are evaluated. Depending on the results of the risk assessment, a due diligence is performed on the supplier.
- Particular care is given to the assessment of intermediaries. Intermediaries are not suppliers and are subject to due diligence with formal assessment and approval, in accordance with the Group policy "Dealing with Business Partners", included in the Compliance Policy 308 of the Compliance Manual. (See standard PC-10-15-030-080)

PC-20-10-040-010

[Risk(s): Business non-compliance; Corruption]

- There are written conditions recorded for each supplier, including a contract and confirmation of main conditions by the supplier.
- These conditions include at least: price list, discounts, volume and/or year-end rebates, payment terms, and also apply to service suppliers, including outsourced delivery. Payment terms must be aligned with local laws and regulations.
- Terms and conditions are regularly updated in the system.
- Contractual conditions are reviewed by the Legal Department and final approval of the supplier is granted by local top management, both in accordance with Group and local Approval Matrices.
- The contract includes a commitment by the suppliers to meet the specific expectations set forth in Sonepar's Business Partners Code of Conduct and to comply with all applicable laws and regulations, contractual obligations and Sonepar policies.
- The Contract is signed by both parties, and supplier-related contracts are recorded in the supplier file and available to local management.

PC-20-10-040-015

[Risk(s): Business non-compliance]

► Control activities are performed to ensure supplier terms such as payment terms, warranties, and insurance are properly applied and that they comply with local laws and regulations.

PC-20-10-040-040

[Risk(s): Access; Corruption]

► There is a formalized procedure for the creation and modification of suppliers.
► For any supplier creation or modification, sensitive information (banking information and payment terms) is confirmed by phone with a known and trusted contact at the supplier's office and this verification process is documented.
► Each change in bank information is promptly validated by an individual who does not have access to modify the supplier database. Additionally, other changes to the Supplier Master File are independently reviewed at least on a monthly basis.
► Access to enter supplier data is restricted by user permissions in the system.
► Associates with access to modify the Supplier Master File are not authorized to initiate payments.
► Associates in charge of modifying the Supplier Master File are trained regularly on potential fraudulent behavior (e.g. Fake president fraud risk, Payment to fake supplier scheme).

ACTIVITIES

Manage tender and selection process

PC-20-10-050-015

[Risk(s): Performance gap; Corruption; Business non-compliance]

► A formal procedure describes the tender process regarding purchases for other than stock inventory (general expenses, services delivery...).
► It includes, at least:
  • The tender process itself with, among others:
    - The definition of a threshold above which a tender process is required
    - The minimum number of suppliers to involve in the tender process
    - The formalization of requirements/specifications that will determine the choice (RFP)
    - The formalization of a comparison table with answers obtained on all appropriate selection/elimination criteria (cost, expertise, timeframe, understanding of needs, feedbacks...), which justifies the final choice
  • The validation process (incl. budget defined and approval matrix applicable and up to date)
  • The legal (e.g. NDA), compliance (e.g. Business Partner Assessment, review of potential conflict of interest), IT security and CSR requirements to be inserted and respected as part of the RFP and the choice of the retained candidate.

ACTIVITIES

Select a supplier

PC-20-10-060-010

[Risk(s): Third-party non-compliance; Corruption; Value chain workers rights]

► Before ordering, it is ensured that policies, procedures and criteria for supplier selection are documented and approved by management, and include expectations of suppliers set forth in Sonepar's Business Partners Code of Conduct.
► Selection of a supplier by management is based on predefined criteria (financial stability, corruption risk assessment...) described in said written policy.
► Management ensures (through contractual clauses and/or Business Partner Assessment) that the supplier will act in accordance with Sonepar commitments and principles, including: respect for Human Rights, prevention of harassment and discrimination, protection of the environment, and operating with business integrity.
► Conflict of interest within the purchasing department are prohibited to avoid uncontrolled procurement.
► An identification and development program of e-capabilities (EDI/web) is also set up and validated by management.

PROCESS:

MANAGE PURCHASE ORDER

ACTIVITIES

Validate purchasing price with the supplier and issue the Purchase Order

PC-20-20-040-010

[Risk(s): Authority/limit; Business non-compliance; Corruption]

- ► An approval matrix (delegation of authority) is set up concerning purchasing rules for other than stock items (general expenses and services delivery) specifying that authorization is needed for purchases above predefined thresholds (quantities or amounts).
- ► Above a threshold predefined by local management, a dual validation is needed.

PC-20-20-040-020

[Risk(s): Authority/limit; Business non-compliance; Corruption]

- ► The purchase price for overhead purchases (general expenses and services delivery) is reviewed and approved in accordance with the approval matrix.

ACTIVITIES

Manage open PO

PC-20-20-060-010

[Risk(s): Performance gap]

- ► Open purchase orders for overhead purchases are reviewed at least monthly to ensure that confirmed suppliers delivery dates are not exceeded.

PROCESS:

FOLLOW VENDORS RELATIONSHIP AND NEGOTIATION

ACTIVITIES

Ensure rebates programs are reviewed

PC-20-30-030-010

[Risk(s): Performance gap; Corruption; Accounting information]

- ► Management approves rebates process and programs to ensure appropriate calculation methodology and rebate structure for each supplier.
- ► Accrued rebates and other receivables from suppliers based on contractual conditions are calculated and reviewed (monitoring of payment and aging of these receivables) on a monthly basis and supported by appropriate documentation.

ACTIVITIES

Follow vendor's obligations and incentives

PC-20-30-040-010

[Risk(s): Performance gap; Corruption]

- ► Controls are made in order to ensure that every service and obligations formalized in suppliers' contracts are properly performed.

ACTIVITIES

Evaluate and monitor suppliers

PC-20-30-050-005

[Risk(s): Business non-compliance; Corruption]

- ► There is a procedure to ensure the following documents are in force:
  - Written conditions for each supplier;
  - Yearly commercial agreements (conditions/rebates/marketing allowances/…);
  - Any specifics items of negotiation.

PC-20-30-050-010

[Risk(s): Performance gap; Dependency; Corruption]

► There is a monthly review by management of the Top 20 purchasing contracts or representing at least 70% of the purchased amounts.
► Suppliers are evaluated following predefined criteria, among them:
- Compliance with Sonepar's Business Partners Code of Conduct, contractual obligations and Sonepar policies;
- Respect of delivery times;
- Quality of the goods delivered;
- Reliability of invoicing;
- Returns policy.

PC-20-30-050-040

[Risk(s): Skills and knowledge capital; Performance gap]

► There is an evaluation of suppliers' support and training programs. Also, it is recommended that:
- the structure of technical training for sales team is optimized by using suppliers support.
- the suppliers training programs lead to distribution label and a certification for our teams.

PC-20-30-050-060

[Risk(s): Performance gap; Corruption]

► Additional services provided to suppliers (including Data monetization) are reviewed by management and properly invoiced. These additional services comply with all Sonepar policies and procedures.

PC-20-30-050-070

[Risk(s): Performance gap; Corruption]

► Sales of services to suppliers (eg. data analysis, delivery offers, storage solutions…) are formalized in a contract approved by management and verified by operational control focusing on coherence of the amounts, reality of the service given, contractual terms etc. Depending of the type of services provided, services must not be deductible from the invoice. The control is performed by someone independent from direct management and purchasing activities.

PC-20-30-050-090

[Risk(s): Accounting information; Performance gap]

► The calculation regarding year-end bonuses is based on the formal conditions defined with suppliers. The amount of year-end bonuses is properly controlled for every supplier.

PC-20-30-050-100

[Risk(s): Third-party non-compliance; Corruption]

► Occasional suppliers are tracked and monitored. The use of occasional supplier has to be validated by management. All policies and procedures applicable to suppliers are also applied to occasional suppliers including but not limited to the Business Partners Assessment policies and procedures.

PC-20-30-050-110

[Risk(s): Performance gap; Business non-compliance]

► Aging balance and trend analysis is reconciled with General Ledger and reviewed by Finance director on a monthly basis.

ACTIVITIES

Monitor SPA

PC-20-30-060-010

[Risk(s): Anti-competitive practice; Performance gap; Business non-compliance]

► A formalized procedure is implemented to govern Special Pricing Agreements (SPA) and to enable clear understanding and processing including:
- Clear definitions of what is locally considered an SPA;
- A detailed list of all types of SPAs and implementation rules for each of them;
- The monitoring process to anticipate their expiration dates;
- The process for booking accruals for debit notes receivable (calculation, collection);

► Access to SPA is secured and restricted to a limited number of associates who have a strict need-to-know.

PROCESS:

MONITOR USER ACCESS

ACTIVITIES

Monitor user access

PC-20-40-010-001

[Risk(s): Access; Authority/Limit]

- Managers are responsible for ensuring that proper segregation of duties is in place. Incompatible duties within the purchasing department (or department in charge of purchases) are segregated (e.g. segregation of duties between purchasing order processing, receipt of goods and payment validation).
- Reviews of access are performed at least on a yearly basis.
- User access to sensitive purchase transactions (Supplier Master Data, billing, returns…) is secured and monitored.

Supply Chain

PROCESS:
PLANNING

ACTIVITIES

Define inventory strategy

PC-30-01-005-010

[Risk(s): Supply/Sourcing; Performance gap]

► Service Level Strategy (SCP Playbook S1)
- The inventory service level parameters must be set to achieve a minimum of 98% overall availability in customer lines, with at least 99.5% on AX SKUs.
- The assortment is categorized and updated monthly using a Pareto logic, considering two criteria: ABC (based on COGS) and XYZ (based on customer sales order lines).

PC-30-01-005-020

[Risk(s): Supply/Sourcing; Performance gap; Customer satisfaction]

► Strategic Forecasting (SCP Playbook S2)
- Forecast accuracy (incl. seasonality when applicable) must be measured monthly to improve customer availability and inventory quality.

PC-30-01-005-030

[Risk(s): Supply/Sourcing; Performance gap; Customer satisfaction]

► Assortment planning (SCP Playbook S3)
- A monthly quantitative analysis must be performed to:
  - review assortment decisions, including the implementation and monitoring of action plans for cleaning up SKUs that are removed from the assortment.
  - support the decision of whether or not to stock an SKU (based on historical data such as the number of unique customers, the number of order lines and turnover).

PC-30-01-005-040

[Risk(s): Supply/Sourcing; Performance gap; Access]

► IMS Settings (SCP Playbook DM2)
- Changes such as service level parameters, holding costs, ordering costs and ABCXYZ classifications are restricted to authorized associates.
- All parameter changes must be simulated before implementation. If there is a significant change, it must be validated by appropriate stakeholders (Finance, warehousing, sales, etc.).

ACTIVITIES

Manage orders

PC-30-01-010-010

[Risk(s): Authority/Limit; Corruption]

► Organization (SCP Playbook SA3)
- An approval matrix for material purchases has to be established to ensure proper authorization for purchase orders that exceed predefined thresholds.

PC-30-01-010-015

[Risk(s): Performance gap; Corruption]

► Price conditions (SCP Playbook DM3)
- Before ordering, the purchase prices must be reviewed and approved and exceptional conditions such as additional discounts, promotions, derogations, etc. must be reviewed by management and properly supported by documentation validated for each supplier.

PC-30-01-010-020

[Risk(s): Performance gap; Customer satisfaction; Supply/Sourcing]

► Open Orders (SCP Playbook D1)
- Open purchase orders for materials must be reviewed daily to ensure that delivery dates are confirmed by the supplier, with particular attention to overdue deliveries or those expected within the next three days.

PC-30-01-010-030

[Risk(s): Supply/Sourcing; Performance gap]

► Phasing in SKUs (SCP Playbook M1)
- Before issuing an order for a phase-in item, return right must have been agreed upon with the supplier.

PC-30-01-010-035

[Risk(s): Performance gap]

► MOQ (Minimum Order Quantity) Management (SCP Playbook Q1)
- Accurate minimums, incremental and packaging information (e.g. lot size, box, pallet configuration) must be checked before issuing a purchase order.

PC-30-01-010-040

[Risk(s): Performance gap]

► Daily Ordering (SCP Playbook D2)

- There is a specific purchasing procedure for non-stock articles (i.e. non frequent articles).
- Controls are implemented on non-stocked orders in order to ensure that:
  - it is related to a customer order,
  - the lead time is respected,
  - the item is not included with other stocked orders (which could result in extending lead times and negatively affect product availability),
  - it can only be placed if the item is not already considered as excess inventory and available in a distribution center or a branch.

PC-30-01-010-050

[Risk(s): Performance gap]

► Managing customer reservation (SCP Playbook D5)

- Effective inventory reservation policies for customer must incorporate clear parameters, such as limits on time, volume, and value limits, to prevent excessive strain on resources.
- Monthly reviews of reservations with sales teams and senior management are conducted to ensure alignment with organizational objectives while maintaining a customer-centric approach.

PC-30-01-010-060

[Risk(s): Performance gap; Performance measurement; Vendor/Supplier relationship]

► Supply Reliability (SCP Playbook D1)

- Supplier lead time accuracy is measured monthly against Group standards, including on-time delivery, in-full delivery and on-time in-full delivery. The results are shared with suppliers and poor performance leads to developing an improvement plan with them.

ACTIVITIES

Analyze and optimize stock level

PC-30-01-020-010

[Risk(s): Performance measurement; Performance gap; Customer satisfaction]

► Monitoring (SCP Playbook DM1)

- The following metrics must be calculated and analyzed monthly per Supplier, Product Category and Location.

  Availability metrics:
  - Line fill rate
  - TLFR (Total Line Fill Rate)
  - List of stockouts

  Inventory quality metrics:
  - Inventory value
  - Inventory value at branch level Vs Total
  - Non stocked Value
  - Overstock value
  - Depreciation
  - Inactive inventory
  - Dead stock
  - Operational DIO

  Assortment metrics:
  - Sales order lines from stocked SKUs %
  - Direct sales Vs total sales %

  Performance metrics:
  - Break bulk ratio
- An analysis is completed (Xray for Slim4) with evaluations performed at least monthly for each SKU, supplier, and product category.
- Inventory cleaning actions are taken in collaboration between the Supply Chain Planning, Category Management, and Purchasing departments.

PC-30-01-020-020

[Risk(s): Supply/sourcing; Performance gap]

► Inventory Allocation (SCP Playbook Q3)

- There is a monthly control in place to ensure that all SKUs stocked in a branch are also be stocked in their associated Distribution Center.

PC-30-01-020-030

[Risk(s): Performance gap]

► Forecast Exception Management (SCP Playbook D4)
- Forecast exception reports (automatically generated) are controlled by planners within the first week of each month.

PC-30-01-020-040

[Risk(s): Performance gap]

► Phasing out SKUs (SCP Playbook M2)
- The Category Management team is supporting the phase-out plan to reach "inventory zero" by the phase-out date with promotions and returns to be applied.
- The Supply Chain Planning team is responsible for developing a phase-out plan that considers the entire distribution network, ensuring that all locations reach "inventory zero" by the phase-out date.

PROCESS:

WAREHOUSING

ACTIVITIES

Manage reception of goods

PC-30-02-010-010

[Risk(s): Performance gap; Misappropriation of assets; Product quality]

► All received goods are inspected (for quality and quantity) and counted upon receipt (by use of comparing packing list, purchase order and goods).

► Reception and shelf placement are done in a timely manner to ensure goods are properly entered into the system and made available for sale.

PC-30-02-010-020

[Risk(s): Performance gap; Misappropriation of assets]

► A procedure is implemented to monitor internal cross docking, including at least:
- controls on quality/ quantities;
- guarantee that all goods incoming into the cross-docking area are leaving in a timely manner;
- respect of deadlines;
- flows regular monitoring.

PC-30-02-010-030

[Risk(s): Accounting information]

► Prevention of back-dated bookings in the IT systems is implemented.

ACTIVITIES

Perform inventory physical counts

PC-30-02-020-010

[Risk(s): Accounting information; Misappropriation of assets; Customer satisfaction]

► Written procedures and guidelines (such as predetermined methods to measure quantities, high-value item counting and unannounced stock counting) are set prior to stocktaking, and are communicated and explained to the warehouse and storage managers. These procedures must include at a minimum the following:
- A copy of the perpetual inventory file is generated before the stocktaking, during which no transactions (in the system or physically) may be performed;
- Counting is performed in a way that ensures proper segregation of duties and four-eyes principle is in place (contact your local internal control or auditor for advice);
- "Blind counting" is performed (system quantities are neither printed on the ticket nor displayed on the screen);
- Count results are re-verified or at least randomly tested: discrepancies are immediately retested and resolved by a supervisor.

PC-30-02-020-020

[Risk(s): Accounting information; Misappropriation of assets; Customer satisfaction]

- ▶ All inventory items (incl. material rented to customers) are physically checked and counted at least once a year, either through a comprehensive physical inventory count or through a thorough and documented cycle count process.
- ▶ Alternative procedures such as those performed by external auditors, are validated, explained and properly documented.

PC-30-02-020-030

[Risk(s): Accounting information; Misappropriation of assets]

- ▶ Items on display, consigned or kept off-site are approved and physically checked each year end (Q4). A wall-to-wall / floor to ceiling complete inspection is also performed each year to verify and count all items on site, including defective goods, special/non stock goods to be returned, will call, etc.
- ▶ Annual verification and validation for off-site inventories not physically performed is required.

PC-30-02-020-040

[Risk(s): Accounting information; Misappropriation of assets; Corruption]

- ▶ Free samples received are placed into stock (quantities and values). There is a formal procedure to monitor free samples, including samples checks upon arrival, valorization methods, movements follow-up, specific warehousing storage areas, etc.

PC-30-02-020-050

[Risk(s): Misappropriation of assets; Accounting information; Customer satisfaction; Corruption]

- ▶ All differences in the quantities of goods when conducting physical inventory and perpetual inventory are documented in a timely manner, investigated and analyzed by warehouse locations / Stock keeping units (SKU) and using the following metrics:
  - error rate: Percentage of shipped orders containing errors or the number of credit memos for incorrect products or quantities, divided by the number of invoiced lines;
  - discrepancy Rate: Percentage of warehouse locations with discrepancies or the number of adjustments made to the perpetual inventory, divided by the number of warehouse locations;
  - zero location control: number of zero locations (IT system) where articles are found, over the total number of warehouse locations or number of counted locations.
- ▶ Differences are reported to OPCO management.

ACTIVITIES

Monitor stock adjustments

PC-30-02-030-010

[Risk(s): Authority/limit; Misappropriation of assets; Corruption]

- ▶ A formalized, approved, and communicated procedure governs stock adjustments and clearly defines required authorization, documentation, processing steps, and responsibilities.
- ▶ Access to perform stock adjustments (quantity and/or value) is restricted to authorized users, and all adjustments are subject to documented management approval.
- ▶ Stock adjustments are fully documented and recorded promptly in the General Ledger to ensure the completeness and accuracy of book inventory and inventory balances.
- ▶ Stock adjustments are monitored at least monthly, by nature, location, product, and responsible individual, using absolute values (exhaustive review of all adjustments whether positive or negative) to detect anomalies, trends or unusual patterns.
- ▶ When stock adjustments are made by management, an independent review by a separate department is performed to confirm accuracy and compliance with established procedures.

PC-30-02-030-020

[Risk(s): Authority/limit; Misappropriation of assets; Corruption]

- ▶ Permission to change product codes or names in the system ("transcoding") is restricted and granted to authorized associates only; the use of this permission is reviewed monthly by an individual who is independent of logistics activities.

PC-30-02-030-030

[Risk(s): Misappropriation of assets; Accounting information; Corruption]

- ► A procedure for scrapping / obsolete inventory including documentation and approval exists, in accordance with local regulations.
- ► Controls of scrapping of materials/ write-offs and related cost are in place.
- ► Scrapping/write-off processes are supported by adequate evidence (e.g. obsolete inventory report, scrapping certificates, usher report...) and approved by duly authorized persons.

ACTIVITIES

Manage goods' returns

PC-30-02-060-010

[Risk(s): Performance gap; Misappropriation of assets]

- ► A procedure is implemented to manage goods returned to suppliers, which includes required documentation, validation and approval process, reimbursement process, adjustments to inventories, choice of specific localization of products to be returned and general ledger entries.

PC-30-02-060-020

[Risk(s): Performance gap; Misappropriation of assets]

- ► Returns of goods from customers are subject to prior formal approval and are processed in a timely manner, based on a formalized procedure.
- ► Adequate quality checks on the physical condition of returned goods are performed before acceptance and are properly documented.
- ► Returns should be defined as a part of commercial conditions, so that customers are clearly informed.

PC-30-02-060-030

[Risk(s): Performance gap; Misappropriation of assets]

- ► A report on the returns (suppliers and customers) is used to track the quantity and value of processed returns. At least weekly, management uses this information to analyze costs, trends, workload and areas for improvement in the returns process. (see Reverse Logistics - SCP Playbook Q2 for suppliers' returns).

ACTIVITIES

Manage the warehouse

PC-30-02-070-030

[Risk(s): Misappropriation of assets; Logistic infrastructure]

- ► Control mechanisms are in place to secure the storage of goods in the right warehouse location (e.g. barcode scanning, weight checking).

PC-30-02-070-040

[Risk(s): Logistic infrastructure; Health and safety]

- ► Control mechanisms are in place to check the stock quality on a regular basis (physical conditions, storage, cleanliness, etc.).

PC-30-02-070-050

[Risk(s): Health and safety; Logistic infrastructure; Misappropriation of assets]

- ► Warehousing process is organized in order to facilitate identification, ensure safety, and efficient access to stock including spare parts, obsolete and /or damaged spare parts, samples, etc.

PC-30-02-070-060

[Risk(s): Site security; Misappropriation of assets]

- ► Access to inventory area is granted only to authorized personnel (both physical access and system access).

PC-30-02-070-070

[Risk(s): Site security; Misappropriation of assets]

- ► Sensitive and damageable products are stored in dedicated and secured areas, handled and kept with extra precaution. For these products, outside storage areas are limited (as much as possible) and specific controls (cameras, patrols…) are implemented in such cases.

PC-30-02-070-080

[Risk(s): Logistic infrastructure]

- ► Products stored outside have to be designed to sustain weather conditions (to respect insurers prerequisites in term of coverage).

ACTIVITIES

Prepare customer order

PC-30-02-080-010

[Risk(s): Customer satisfaction]

- ► There is a formalized procedure describing customer order preparation's process.
- ► Controls are performed while preparing customer orders to ensure quality requirements are met.

PC-30-02-080-020

[Risk(s): Customer satisfaction; Performance gap]

- ► There is a monthly monitoring of customer order preparation quality and effectiveness, including:
  - Total number of order lines containing errors (wrong articles, missing articles, wrong quantity, damaged, delivered to the wrong address) / total number of order lines shipped by the warehouse (logistic error rate);
  - Number of customer claims received / total number of outgoing lines, relating to Incorrect article or error in quantity or damage during transport or delivery delay;
  - Number of ordered lines shipped / total person-hours expended in the warehouse is calculated and analyzed.

PROCESS:

TRANSPORT

ACTIVITIES

Manage transport activity

PC-30-03-010-001

[Risk(s): Performance gap]

- ► Transport costs are monitored and reported according to the Group Transport Cost Guide Handbook.
- ► In particular, there is a specific follow-up regarding express transport required by customers.
- ► The following Transport Cost KPIs must be measured and managed in alignment with the Group definitions on a at least monthly basis:
  - Transport Cost per Distributed Orders;
  - Transport Cost per Stop;
  - Transport Cost per Kilometer or Mile;
  - Transport Cost per Shipping Units;
  - Transport Cost per Distributed Orders after Monetization.
- ► Transport Cost in value and as a percentage of sales must be reported via the Group Cost By Function reporting process.

PC-30-03-010-010

[Risk(s): Third-party non-compliance; Corruption; Performance gap]

- ► The choice of carriers is made following a formalized tender process. Criteria such as quality, volume possibilities, tariffs, Business continuity of the carriers and respect of environmental factors must be included.

PC-30-03-010-020

[Risk(s): Third-party non-compliance]

- ► Contracts with carriers are formalized and reviewed by legal, HR and Finance departments, to include alignment with local transport and social regulations and laws (responsibilities, penalties, fines, taxes, environmental restrictions, long hours restrictions, day/night shifts rules…), as well as code of conduct, tariffs and penalties, claims, services agreements, insurances policies, privacy policies and active Business Continuity Plan.

PC-30-03-010-030

[Risk(s): Business non-compliance; Labor laws; Performance gap]

- ► At country level (or if appropriate at OPCO level), a local transport and drivers policy is established to outline the following:
  - appropriate working environment for transport, including the selection of internal or external drivers, leased or owned trucks etc.;
  - local legal and social regulations including sustainability requirements;
  - scope of responsibilities (e.g. for maintenance, casualty handling, fines etc.…);
  - transport order flow process;
  - robust transport planning including transshipment points, in cases where the transport is not dedicated, meaning it carries products from other sources and not only Sonepar products, whether operated by third parties or own transport;

- delivery standards;
- insurance requirements;
- cost allocation for fuel expenses;

► This policy is reviewed by Human Resources, Legal and Finance departments and validated by the Supply Chain Director.

PC-30-03-010-040

[Risk(s): Performance gap; Business non-compliance; Customer satisfaction]

► SLAs (service level agreements) are formally established with carriers and/ or company's own transport fleet.

► Deviations from the established SLAs are documented, analyzed, and corrective actions are taken to ensure the service level is consistently maintained.

► The performance of carriers or company's own transport fleet is evaluated periodically, taking into account the SLA results including delivery and dispatch time, number of routes used, customer satisfaction, and any other relevant metrics.

► Monthly monitoring results are shared with carriers and company's own transport fleet, to drive continuous improvement , and to make informed decisions for future partnerships and agreements with carriers.

ACTIVITIES

Manage shipment

PC-30-03-020-010

[Risk(s): Performance gap; Customer satisfaction]

► There is a formal procedure for controls to be performed on shipments (e.g. physical inspection, match versus order information, freight document correctness, etc.).

PC-30-03-020-020

[Risk(s): Misappropriation of assets; Access]

► The shipping data (specifically, the customer delivery address) in the IT system can be modified only by a limited number of authorized associates.

PC-30-03-020-030

[Risk(s): Accounting information]

► All shipments are timely entered and recorded into the system, to ensure inventory is released and sales are properly booked.

ACTIVITIES

Ensure customer's delivery

PC-30-03-030-010

[Risk(s): Misappropriation of assets]

► Logistic personnel ensure that customers check the goods and sign the packing slip for acceptance, unless there is a contract stating otherwise (like overnight deliveries/ drop in by the shipping company…).

PROCESS:

MONITOR LOGISTIC ACTIVITIES

ACTIVITIES

Follow supply chain analytics

NEW PC-30-04-005-010

[Risk(s): Performance measurement; Performance gap]

► Supply chain Analytics KPIs defined in the new reporting framework (incl. KPIs definition in appendices) are calculated, analyzed and reported on a monthly basis.

ACTIVITIES

Monitor user access

PC-30-04-010-010

[Risk(s): Access; Authority/limit]

► Managers are responsible for ensuring proper segregation of duties are in place and regular access reviews are performed. User access to sensitive logistics transactions (stock movements, stock adjustments, procurement...) are secured and monitored.

Merger & Acquisition

The Acquisition Manual reflects the Group governance through the Acquisition process.

It shows Sonepar's expertise acquired through the years, best practices, guidelines, tools and templates to continue making successful acquisitions from the definition of the strategy at country level to the completion and full integration into Sonepar businesses.

PROCESS:

MAINTAIN AN ACQUISITION STRATEGY AND PROCEDURES

ACTIVITIES

Maintain market watch and strategy

PC-40-10-010-010

[Risk(s): Acquisition; Competition]

► There is an active and formalized market watch activity in the organization to identify potential acquisition targets.

PC-40-10-010-020

[Risk(s): Acquisition]

► Acquisition strategy and target list are approved by Group Management as a part of the multi-year strategic plan.

ACTIVITIES

Maintain procedure awareness

PC-40-10-020-010

[Risk(s): Acquisition]

► Local management is aware of the Group acquisition governance and process including the Acquisition Manual.

ACTIVITIES

Ensure legal confidentiality

PC-40-10-030-010

[Risk(s): Acquisition; Business non-compliance]

► Confidentiality agreements are systematically signed at the beginning of a M&A project. Confidentiality is also systematically covered in the letter of intent or indicative offer as well as in sale and purchase agreements.

► In large and/or sensitive acquisitions/divestments, internal confidentiality letters are prepared and signed by all involved associates.

PROCESS:

IDENTIFY TARGET AND EXPLORATORY PHASE

ACTIVITIES

Assess culture fit

PC-40-20-010-020

[Risk(s): Acquisition]

► Group acquisition process and relevant information are available to the project team to explain Sonepar culture to the target.

ACTIVITIES

Assess target financials and risks

PC-40-20-020-010

[Risk(s): Acquisition; Business non-compliance; Performance gap]

► All pre-acquisition controls (double accounting, non-audited accounts, …) are performed, documented and communicated to the Investment committee and Management in order to make sure that the target does not have any deviant practices or is in a country excluded from the Group list.

PROCESS:

PREPARE DOCUMENTATION FOR THE INVESTMENT COMMITTEE

ACTIVITIES

Prepare business case

PC-40-30-010-010

[Risk(s): Acquisition]

► The business case template available in appendix to the Acquisition Manual has been made available to the project team.

PC-40-30-010-020

[Risk(s): Acquisition]

► The business case is prepared by the project team and signed by the local top manager.
► It includes :
- Synergies and opportunities definition;
- A legal, risk and compliance assessment (including code of conduct and policies);
- A review of insurances coverages and potential claims;
- Strategic valuation of the target and identification of the key potential risks;
- An integration plan (including IT, if applicable).

► The business case is documented and sent to the Investment Committee.
► Authorization from the Investment Committee is obtained prior to signing a letter of intent or an indicative offer.

ACTIVITIES

Prepare acquisition sheet

PC-40-30-020-010

[Risk(s): Acquisition; Business non-compliance]

► Before signing the letter of intent and starting the due diligence, a clear assessment has been done to determine whether the acquisition will need to be notified and/or approved by a competition authority.

PC-40-30-020-020

[Risk(s): Acquisition]

► The acquisition sheet template available in appendix to the Acquisition Manual has been made available to the project team. It is completed by the project team and signed by the local top manager then sent for review and approval by the Investment Committee.

PC-40-30-020-030

[Risk(s): Acquisition]

► The accuracy of the financials provided to elaborate the acquisition sheet is challenged and documented.

ACTIVITIES

Prepare the due diligence team

PC-40-30-030-010

[Risk(s): Acquisition]

► As mentioned in the Acquisition Manual and in the Compliance Manual, a "Clean Team" must be set up before sharing any competitively sensitive information to avoid any competition distortion. Each Clean Team member must sign a Clean Team Non-Disclosure Agreement.

PROCESS:

CONDUCT DUE DILIGENCE ON THE TARGET

ACTIVITIES

Challenge the information provided during the due diligence

PC-40-40-010-010

[Risk(s): Acquisition]

► The accuracy of the operational, commercial, financial, HR, legal and tax information provided during due diligence are challenged and documented.

PC-40-40-010-050

[Risk(s): Acquisition; Performance gap]

► A gap analysis between the target and Sonepar's standards is prepared and shared with management and the Investment Committee.

PC-40-40-010-060

[Risk(s): Acquisition]

► Red flag due diligence report including all the high risk items is formalized, attached to the acquisition sheet and sent to the Investment Committee for review.

ACTIVITIES

Review financial, tax, operational, legal, compliance, IT and HR aspects / status of the target

PC-40-40-020-010

[Risk(s): Acquisition]

► The choice of the local legal external advisor is made with the approval of Sonepar General Counsel. Sensitive projects are selected in coordination with HQ, finance and legal departments. Due diligence checklist available in appendix of the Acquisition Manual are systematically used. Projects are reviewed by the Investment Committee in accordance with the Acquisition Manual.

PC-40-40-020-020

[Risk(s): Acquisition]

► The decision on the most suitable legal structure to adopt for the acquisition is documented, shared and approved by Sonepar General Counsel.

PC-40-40-020-030

[Risk(s): Acquisition]

► The contract includes all provisions necessary to protect Sonepar's interests such as a clear calculation formula in case of future earn-outs, representations and warranties.

PC-40-40-020-040

[Risk(s): Acquisition]

► Legal documentation concerning the operation has been reviewed by the Country Head of Legal as well as the Region Head of Legal and/or Group legal department.

ACTIVITIES

Anticipate integration steps

PC-40-40-030-010

[Risk(s): Acquisition]

► Prior to closing, integration governance and relevant resources (integration leader and members of the steering committee) are identified and communicated to the Investment Committee.

PROCESS:

FINALIZE LEGAL DUTIES AND COMMUNICATE ABOUT THE DEAL

ACTIVITIES

Finalize legal duties

PC-40-50-010-010

[Risk(s): Acquisition; Authority/limit]

► Before signing of the sale and purchase agreement, all steps have been completed and all approvals have been obtained in compliance with the Acquisition Manual and the Approval Matrix.

PC-40-50-010-020

[Risk(s): Acquisition; Authority/limit]

► Investment Committee's approval is documented before signing the sale and purchase agreements.

ACTIVITIES

Communicate the deal

PC-40-50-020-010

[Risk(s): Acquisition; Communication]

► A clear internal and external communication plan is developed, sent at the latest 48h before the publication, and approved by the Chief Communication Officer.

PROCESS:

FOLLOW THE INTEGRATION OF THE ACQUISITION WITHIN THE GROUP

ACTIVITIES

Follow the integration of the acquisition

PC-40-60-010-010

[Risk(s): Acquisition; Post-merger large integration; Performance gap]

► As outlined in the Acquisition Manual, for each acquisition, as part of the governance of the integration, an integration leader is designated early on and presented to the Investment Committee.

► He/she will be responsible for:

- coordinating and centralizing all requests from the HQ, the region and the country to the new business;
- sharing on a regular basis a roadmap of the integration process with the new business (ranked by tasks with completion date objectives);
- monitoring the pre- and post-acquisition checklists;
- managing the operational integration.

PC-40-60-010-020

[Risk(s): Acquisition; Corruption]

► There is a post cash-out check, performed by Finance department, to verify that no fees or undue moneys/ compensation have been paid to facilitate the acquisition (via fees for example).

PC-40-60-010-030

[Risk(s): Acquisition; Post-merger large integration]

► For all density acquisitions, the integration assessment questionnaire must be completed at the latest 12 months after the acquisition closing date and sent to HQ M&A team.

Finance & Accounting

PROCESS:

PREPARE AND APPROVE BUDGET

ACTIVITIES

Prepare and approve budget and forecasts

PC-50-10-010-020

[Risk(s): Budget & planning]

► Annual budget and the 2 yearly forecasts are coordinated by Finance Department, communicated to the Group executive management for confirmation of the objectives, and approved by the Board of Sonepar based on information provided by branches / OPCO.

ACTIVITIES

Manage investments

PC-50-10-020-010

[Risk(s): Authority/limit; Budget & planning]

► There is a request for approval investment policy in force indicating the applicable threshold according to Sonepar approval matrix. Below corporate thresholds, approval levels are defined in local policies according to Sonepar approval matrix.

PC-50-10-020-020

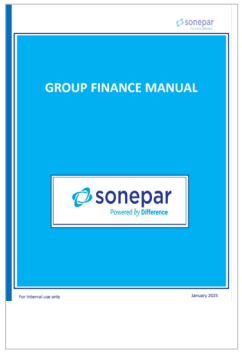
[Risk(s): Authority/limit; Budget & planning]

► According to the RFA guidelines, all RFAs have to be submitted via the official RFA tool (available on the intranet).
► All investments above RFA thresholds (Opex, Capital expenditures, leasing obligations...) are reviewed by country operational and finance leaders and validated by local and regional management (including profitability analysis, P&L, Discounted Cash Flow).
► According to thresholds and categories, after validation at country level, projects must be aligned, validated and approved by Group functional leaders and/or by Group investment committee.

The Sonepar Request for Approval (RFA) process' guideline is a global standard operating procedure for investments that require Group approval.
It supports the Sonepar transformation, while considering local priorities. It streamlines the investment decisions and ensures:
- Modernization and standardization of our IT solutions and Supply Chain assets
- Convergence of our tools and processes and accelerated adoption
- Group leverage, creation of synergies and increased profitability
- Alignment with our Group strategy, Impact plan and long-term objectives
- Full integration with our compliance guidelines and approval thresholds

PROCESS:

MANAGE ACCOUNTING ACTIVITIES



The Finance Manual gathers the Group standards rules for preparing and overseeing the companies' financial statements.
The reporting principles adopted by Sonepar are the International Financial Reporting Standards (IFRS). Therefore, accounts prepared and reported to Group by OPCOs must be compliant with IFRS.
This manual, along with the Group consolidation and reporting tool (SWITCH), ensures consistency and standardization across Sonepar.

ACTIVITIES

Process accounts receivable

PC-50-15-020-010

[Risk(s): Misappropriation of assets; Financial reporting; Corruption]

- Cash receipt, bank deposits and remittance advices are reconciled with the GL in a timely manner by Finance Department / adequate associates; all discrepancies (unapplied cash / customer complaints) are reviewed and corrected by Finance Department.

ACTIVITIES

Process accounts payable

PC-50-15-030-005

[Risk(s): Misappropriation of assets; Corruption; Authority/limit]

- Before processing payment, there is a three way match control in place to confirm alignment between the invoice, purchase order, and delivery receipt.
- For non trade items if no PO exists, invoices must be matched against appropriate supporting documentation, such as contracts, agreements, or approved requisitions, to confirm the transaction's validity.
- Controls of purchase orders and reception discrepancies are duly performed by the accounting department in order to prevent corruption risk between an associate of the accounts payables department and a supplier.

PC-50-15-030-010

[Risk(s): Misappropriation of assets; Financial reporting; Corruption]

- There is a procedure formalizing that payments are processed by the finance department only after invoice accuracy and validity have been verified.
- Payments are processed within agreed payment terms, and periodic reviews ensure compliance with local regulations.
- There is a systematic segregation of duties between the individual initiating the payment on the platform (Electronic banking system or treasury management system) and the individuals signing the payment.
- Administrators of the treasury management and accounting systems are not the individuals initiating or signing payments nor the individuals booking the transactions in the ERP.

NEW **PC-50-15-030-020**

[Risk(s): Misappropriation of assets; Authority/limit; Corruption]

- ► Manual payments initiated directly on the Electronic banking system are limited and restricted.
- ► There is a dedicated procedure, specifying the associates able to perform such transactions, the systematic double-validation process and the authorized thresholds.
- ► A formal and independent control of these manual payments is performed at least on a yearly basis.

ACTIVITIES

Control fixed assets

PC-50-15-050-020

[Risk(s): Misappropriation of assets; Accounting information]

- ► Financial Department validates that all recorded assets are supported by appropriate documentation:
  - date of acquisition;
  - price of acquisition;
  - depreciation rate (depending on asset category);
  - location;
  - registration number;
  - gross booked value.
- ► Assets in progress are regularly checked and are reviewed on an annual basis to check for any loss of value.
- ► Any change of assets is documented and approved.
- ► Unused assets are identified and isolated.
- ► Capital removal (transfer, destruction, disposal or sale) is validated by appropriate management. A certificate shall be signed by the relevant person for each asset destruction or sale.

PC-50-15-050-030

[Risk(s): Accounting information]

- ► Fixed assets' depreciation (rates and methods) are calculated on a monthly basis by Finance Department and reviewed by Finance Manager in accordance with Sonepar principles.

PC-50-15-050-040

[Risk(s): Accounting information]

- ► Intangible and tangible assets are tested for possible impairment according to the Group Finance Manual at least annually, or in the event of a possible loss of value, and validated by Finance Manager.

PC-50-15-050-050

[Risk(s): Misappropriation of assets; Accounting information]

- ► Based on a local procedure, a physical inventory of fixed assets is performed in all entities.
- ► Supply Chain assets in Branches and CDCs (e.g. forklift trucks, machinery...) and sensitive assets (e.g. cars, fixed IT assets...) are counted at least on a yearly basis.
- ► Discrepancies are identified and investigated.
- ► Additional depreciation is booked in case of impairment (good damaged, not in use) after validation from the relevant Finance Manager.

PC-50-15-050-060

[Risk(s): Accounting information; Budget & planning]

- ► Activity recorded in Fixed Assets sub-ledger is reviewed monthly at each place of business by management, including comparison to the capital expenditure budget (divided at least in the following categories: real estate / information systems / transport / equipment / others).
- ► Management issues reports following the review of fixed assets that were performed in order to determine if assets should have been capitalized.
- ► Management must ensure that the information related to CAPEX communicated to the Group under the EU Taxonomy Regulation is complete and reliable.

ACTIVITIES

Review leases

PC-50-15-060-010

[Risk(s): Accounting information]

- ► All real estate leases are reviewed by the Finance manager before signature of leasing contract as per Sonepar approval matrix.

PC-50-15-060-020

[Risk(s): Misappropriation of assets; Authority/limit]

► A policy is established to define the leasing and use of company cars as per Sonepar approval matrix.

ACTIVITIES

Establish accruals, provisions and off-balance sheet commitments process

PC-50-15-070-010

[Risk(s): Accounting information]

► Accruals, contingent liabilities and deferred costs are prepared by Finance Department and reviewed by Finance Manager before monthly closing.
► Reserve requirements and adjustments are made to the month-end closing checklist with at least:
- cut-off related to each operating cycle (notably recording of all delivery notes -from suppliers and to customers);
- goods shipped / received without invoice;
- allowance for doubtful accounts;
- amounts to be received from suppliers;
- inventory write-downs;
- staff costs.

PC-50-15-070-020

[Risk(s): Accounting information; Performance gap]

► Every 3 months, purchasing department reconciles actual purchases data and negotiated agreements with supplier to document accrued year-end bonuses. Bonuses are validated by the finance department.

PC-50-15-070-030

[Risk(s): Accounting information; Performance gap; Corruption]

► There is a formal review and approval of customer rebates to be credited by someone independent from sales activity.
► There are controls over outstanding/overdue balance in place before crediting the rebate.
► There is a review of the customer year-end rebate eligible on collected sales.

PC-50-15-070-040

[Risk(s): Accounting information]

► Off-balance sheet commitments are identified by Finance Department and reviewed by management at least quarterly.
► Specifically, the Finance Department updates the OPCO's bonds and guarantees portfolio using the group's tool, Sonebonds, and ensures/is responsible for its exhaustivity and accuracy.

PC-50-15-070-050

[Risk(s): Accounting information]

► The stock depreciation (incl. scrapping) is calculated monthly and individually according to Sonepar principles / Finance Manual.
► Stock provision is reviewed monthly.
► The Net Realizable Value (NRV) test is performed at year end, as defined in the Group Finance Manual. Depreciation resulting from the NRV test should be recorded in the stock depreciation account.

PC-50-15-070-055

[Risk(s): Accounting information; Misappropriation of assets]

► Stock items with zero value are reviewed at least on a monthly basis and appropriate actions are undertaken.

PC-50-15-070-060

[Risk(s): Accounting information]

► Statistical trade receivable provision is calculated and reviewed monthly according to Sonepar principles / Finance Manual.

PC-50-15-070-070

[Risk(s): Accounting information]

► Doubtful accounts provision is calculated, reviewed and documented on a monthly basis by management, according to Sonepar Finance Manual.

PC-50-15-070-080

[Risk(s): Accounting information]

► Write-offs are validated by management at each occurrence.
► Write-offs are communicated to accounting department for tax recovery purposes with supporting documentation as required by country laws and

regulations (and in accordance with Sonepar Finance Manual).
- ► Management ensures that insurance contract obligations are properly respected.

ACTIVITIES

Close the books

PC-50-15-080-010

[Risk(s): Accounting information]

- ► Procedures or checklists applicable to closing activity are adequate and updated by the finance department.
- ► At least quarterly, the documentation maintained for the closing process and financial reporting is reviewed and approved by the Finance manager.
- ► Financial statements (P&L and balance sheet) are approved by the finance department before month-end close.
- ► Accounting practices and measurement rules are validated by the relevant finance manager according to Sonepar standards and local regulations.
- ► Deviations are identified, adjusted and approved by Sonepar top management.

PC-50-15-080-020

[Risk(s): Accounting information]

- ► A duly approved maintenance form is required for all additions and changes made in the local Chart of Accounts and are properly mapped with the Group Chart of Accounts.
- ► Verification steps are included on the form for business needs and a review is done to ensure no existing account is already in place.

PC-50-15-080-040

[Risk(s): Accounting information; Authority/limit; Corruption]

- ► General Ledger accounts are reconciled with sub-ledgers totals (Accounts Receivable, Accounts Payable, Stocks, Fixed Assets, Payroll) every month and reviewed by the finance department. The reviewer is different from the preparer.
- ► Reconciled items are identified, resolved and reviewed by the finance department on a monthly basis.

PC-50-15-080-042

[Risk(s): Accounting information; Taxation]

- ► Intercompany transactions and balances are validated and reconciled with the related parties and reconciled with the GL.

PC-50-15-080-043

[Risk(s): Accounting information; Corruption]

- ► The suspense accounts are reviewed monthly by Finance Department.
- ► All unusual items or items not associated with rounding errors are investigated and justified.

PC-50-15-080-045

[Risk(s): Accounting information]

- ► IFRS reporting to the Group and statutory accounts (local GAAP) are formally reconciled and reviewed by the local CFO on a regular basis and at least for the year end closing. Reconciling items and adjustments are documented and validated. Special attention is given to any potentially new IFRS requirement, to any exceptional operation and/or change in scope (as explained in the Finance Portal / Group Finance Framework / Change in scope).

PC-50-15-080-070

[Risk(s): Accounting information]

- ► The inventory valuation formula is checked for compliance with Group rules (as outlined in Sonepar Finance Manual) and for proper implementation. This verification must be conducted by associates independent from operations (2nd level control) and once a year by auditors independent from management (3rd level control).

PC-50-15-080-090

[Risk(s): Accounting information; Corruption]

- ► All manual journal entries are reviewed and approved by appropriate level of management.
- ► An in-depth analysis of these manual journal entries is performed at least annually, if possible using data analysis techniques or through the external auditors' review, to identify any discrepancies.
- ► Significant accounting estimates, unusual transactions and non-standard manual journal entries are reviewed and approved by executive management.

PC-50-15-080-100

[Risk(s): Misappropriation of assets; Corruption; Accounting information]

► There are specific controls applicable to transactions performed during the week-end, public/ bank holidays or during particular/unusual times.

ACTIVITIES

Manage bank reconciliations

PC-50-15-085-010

[Risk(s): Accounting information; Corruption]

► Bank reconciliations are reviewed at least on a monthly basis and signed within 5 business days by the Finance Manager:
- reviewer is different from the preparer;
- preparer is not in charge of payments or receipts;
- discrepancies between accounting and bank statement must be resolved within two months;
- documentation (including copies of bank statements) is kept on file in accordance with established record retention policies.

ACTIVITIES

Manage SPA accounting process

PC-50-15-090-010

[Risk(s): Accounting information; Performance gap; Anti-competitive practice]

► Procedures for booking, accounting and reporting of Special Price Agreement activities are documented and up-to-date:
- All general ledger journal entries related to SPA are reviewed and authorized by appropriate associate;
- A formal monthly closing process with documented cut-off procedures for SPA exists;
- A control of the aging of open SPA related debit notes receivable for the duration of the SPA is performed;
- An evaluation of the risk of potential unrecoverability with documentation is realized.

PROCESS:

PREPARE AND APPROVE REPORTING OF ACTIVITY

ACTIVITIES

Prepare and approve reporting

PC-50-20-010-010

[Risk(s): Accounting information; Financial reporting]

► Reporting of activity is accurate, completed in a timely manner on a monthly basis and validated by each level of Management (branch / OPCO / country / Group), in compliance with the Finance Manual.
► A quarterly Cost By Function report is performed, analyzed and uploaded in Switch, according to Group guidelines.
► On a yearly basis, impairment tests' results and additional notes are reported to the Group, as defined in the year-end Group instructions.

PC-50-20-010-020

[Risk(s): Accounting information; Financial reporting]

► A reconciliation of the sum of branches reporting with the OPCO's P&L is performed by Finance Department.
► Reporting to Group level is reconciled with General Ledger by Finance Department.

PC-50-20-010-030

[Risk(s): Accounting information; Financial reporting]

► Every month, Finance team, together with with the branch manager, performs the following analysis, using the Group templates 'Branch URS' and 'Margin Control Report':
- a. analytical review of P&L and Balance Sheet (actual figures vs. last year / budget);
- b. Non-financial data analysis (number of associates (Full Time Equivalent); number of working days for the reporting period);
- c. Ratios analysis (turnover per working day, gross profit per associate, staff expenses/gross profit, total/gross profit, EBIT/local assets);
- d. Gross Profit reconciliation and comments.

► Deviations are reviewed and addressed, at least every 3 months, by the

branch manager together with the OPCO controller / Finance Director.

ACTIVITIES

Perform reviews of specific accounts

PC-50-20-030-040

[Risk(s): Corruption; Accounting information]

- ► According to compliance procedure and requirements, dedicated P&L accounts are created and used to book the following costs:
  - fees and commissions;
  - donations;
  - sponsorship;
  - events and invitations;
  - gifts and gratuities.
- ► These accounts are controlled every month by finance/business controllers.
- ► Unusual transactions and/or amounts are promptly reported to Country CFO, who is responsible to inform Region and Sonepar CFO.

PC-50-20-030-050

[Risk(s): Corruption; Third-party non-compliance]

- ► A control is performed on the specific third-party accounts (Intermediaries, third parties domiciled in high-risk countries, etc.) to verify that transactions carried out with these third parties are valid and supported by an appropriate business justification.
- ► Specific supplier accounts are identified. Transactions posted to these specific accounts are monitored and reviewed monthly by finance and business controllers.
- ► Unusual transactions and/or amounts are promptly reported to the Country CFO, who informs the Region and the Sonepar CFO.

PC-50-20-030-070

[Risk(s): Corruption; Accounting information]

- ► Anti-corruption accounting control plan: There is a formal plan of accounting controls that need to be conducted to prevent the corruption risk (see appendices). This plan includes all controls that cover risks identified in the local risk corruption mapping, defining for each of them its objective, frequency and owner.

PROCESS:

MANAGE FINANCING ACTIVITIES

Group Treasury has designed a formal document gathering guidelines, rules and procedures to help countries and OPCOs to promote prudent financial risk management.

It covers, among others: cash management and financing policy; bank relationship management; payments securitization; foreign exchange, interest rates and commodities hedging policy; treasury investment policy; and financial systems administration.

ACTIVITIES

Implement local debt agreement

PC-50-30-010-010

[Risk(s): Performance gap; Authority/limit]

- ► As mentioned in the Financing, treasury & systems procedures manual, all financing operations are reviewed by Group Treasury, validated by local board in accordance with corporate governance, and implemented locally under the supervision of Group Treasury.

PC-50-30-010-020

[Risk(s): Currency]

- As mentioned in the Financing, treasury & systems procedures manual, all local financing agreements are contracted in the local currency of the OPCO and validated by Group Treasury, unless a specific rationale (tax, natural hedge, etc.…) dictates otherwise.

PC-50-30-010-030

[Risk(s): Financial instrument]

- As mentioned in the Financing, treasury & systems procedures manual, the OPCO neither grants any security, nor makes any pledges to banks to get local financing, unless specific approval is given by Sonepar CFO.

PC-50-30-010-040

[Risk(s): Financial instrument]

- As mentioned in the Financing, treasury & systems procedures manual, when local financings are in place, the Finance Department will always request the provision of a letter of awareness issued by Sonepar Treasurer and signed by Sonepar CFO.

ACTIVITIES

Manage bank relationships and bank accounts

PC-50-30-050-010

[Risk(s): Authority/limit]

- Bank accounts are opened only with banks validated by Group Treasury.
- Local Finance Department regularly monitors the number of its bank accounts to limit the number of banks used. Once a year, the list of open bank accounts per OPCO is shared with the Group Treasury for coherence review purposes.
- Whenever a change of bank details is requested, the new bank details are systematically checked either through a dedicated bank details validation tool (preferred solution) or through a counter-call procedure managed by a person that is neither part of the accounting/treasury team nor the person requesting the payment.
- Bank signing authority documentation for paper and electronic transactions is kept in the entity's records.
- A list of the authorized signatories is kept in the entity's records, updated and communicated to the relevant banking partners, as soon as practically feasible after a change.
- Finance Manager ensures that one GL account is created for each bank account.

PC-50-30-050-020

[Risk(s): Financial instrument]

- Finance Department maintains no more than two banks validated by Sonepar Treasury department. Any exception beyond two banks requires a documented derogation, duly justified and formally authorized by Sonepar Treasury department.

ACTIVITIES

Control bank fees

PC-50-30-060-010

[Risk(s): Performance gap]

- Fees invoiced or debited by banks are checked by Finance Department on a regular basis. Fees applied by banks are consistent with conditions negotiated by Group Treasury or the OPCO (when no cash pooling is in place).

ACTIVITIES

Identify and define foreign exchange exposure

PC-50-30-070-010

[Risk(s): Currency]

- At the time of defining its Budget, each OPCO's Finance Department identifies and defines its foreign-exchange exposure (or updates it relative to the previous year's exposure) and enters it in Switch/BFC.
- At times of budgetary updates (F1 and F2), and between such periods, each OPCO's Finance Department is responsible for monitoring this exposure and notifying Group Treasury in the event of significant deviations.

► During the course of the year, the Finance Department immediately notifies Group Treasury each time a foreign-exchange exposure reaches 1 m€ or more (whether new or changed). As mentioned in the Financing, treasury & systems procedures manual, the Finance department will then access to the Group FX trading platform and adjust its hedging strategy or alternatively inform Group Treasury department (if needed).

ACTIVITIES

Manage foreign exchange hedging

PC-50-30-080-010

[Risk(s): Currency]

► Exposure vs. Hedging:

- As mentioned in the Financing, treasury & systems procedures manual, when annual FX exposure exceeds EUR 5M, OPCO CEO must approve hedging principle prior to implementation of any hedging. Below EUR 5M, OPCO CFO must approve the hedging principle.
- Upon implementation of a hedging strategy, each OPCO's Financement Department monitors the consumption of such hedges vs its identified exposure at least on a monthly basis and exchanges with Group Treasury department in case of significant deviations.

PC-50-30-080-020

[Risk(s): Financial instrument]

► As mentioned in the Financing, treasury & systems procedures manual, below a EUR 30K unit threshold, only spot transactions (no derivatives) are implemented.

PC-50-30-080-030

[Risk(s): Financial instrument]

► As mentioned in the Financing, treasury & systems procedures manual, hedging derivatives are implemented only through the Group FX trading platform. Any derogation requires Group Treasury validation. Any decision of no hedging is duly justified to Group Treasury.

ACTIVITIES

Manage interest rate hedging

PC-50-30-090-010

[Risk(s): Interest rate]

► As mentioned in the Financing, treasury & systems procedures manual, there is no local interest rate hedging (only at Group level).

ACTIVITIES

Manage cash investments

PC-50-30-100-010

[Risk(s): Financial instrument]

► As mentioned in the Financing, treasury & systems procedures manual, cash is centrally managed and therefore exclusively invested internally through current accounts or intragroup loans/borrowings with the Group Treasury department; otherwise a specific derogation must be given by Group Treasury department.

PC-50-30-100-020

[Risk(s): Financial instrument]

► As mentioned in the Financing, treasury & systems procedures manual, cash investments must remain liquid investments with a maturity that will not exceed three months that meet the criteria for classification as cash and cash equivalents, and be classified by auditors accordingly.

ACTIVITIES

Manage factoring activity

PC-50-30-110-010

[Risk(s): Financial instrument; Authority/limit]

► Factoring and securitization transactions require prior authorization from the SVP Financing & Treasury.

PC-50-30-110-020

[Risk(s): Financial instrument; Authority/limit]

► Reverse Factoring facility:
- before any recourse to reverse factoring, SVP Financing & Treasury's validation is required (incl. review of market practice, profitability etc.);
- local Finance department reviews at least once a year that it has systematically paid the bank at the maturity of the invoice and never postponed payment after such date;
- local Finance department checks on a monthly basis that the discounts granted by suppliers are sufficient to at least compensate the cost of financing supported by the OPCO. The control is carried out supplier by supplier in order to identify and implement quickly a corrective action (increase of discount, renegotiation of financial cost, reduction of financing period granted to supplier, revocation of the agreement with supplier) when profitability is not satisfactory.

ACTIVITIES

Manage financing limits

PC-50-30-120-010

[Risk(s): Financial instrument]

► As mentioned in the Financing, treasury & systems procedures manual, in case the limit of annual financing (internal and external) is exceeded during the year, local Finance department provides Sonepar Group Treasury department with an analysis. Financial limit can then be adjusted subject to Region CFO's prior authorization.

ACTIVITIES

Anticipate cash flows

PC-50-30-130-010

[Risk(s): Performance gap]

► As mentioned in the Financing, treasury & systems procedures manual, when the company is part of the cash pool, daily forecasts are provided to Sonepar Treasurer through KTP Web according to Sonepar Treasury guidelines. In case the forecast is not correct, an update is made in KTP Web.

PC-50-30-130-015

[Risk(s): Budget & planning; Performance gap]

► As mentioned in the Financing, treasury & systems procedures manual, a cash forecast is prepared, approved and regularly monitored and updated in accordance with the financial and operating budget allocated by finance department.

PC-50-30-130-020

[Risk(s): Financial instrument]

► As mentioned in the Financing, treasury & systems procedures manual, when an intragroup loan comes to maturity or when a new loan is requested, the company anticipates the refinancing by informing Sonepar Treasurer through KTPWeb according to Sonepar Treasury guidelines.

ACTIVITIES

Manage payment means and treasury

PC-50-30-140-010

[Risk(s): Misappropriation of assets]

► As outlined in the Financing, treasury & systems procedures manual:
- Cash funds, cash receipts, cash disbursements, and cash deposits are managed with appropriate security measures for the cash box/safe and include mandatory controls (such as reconciliations).
- Cash transaction logs (daily cash in/cash out or equivalent digital records) are monitored daily by the local associate in charge, monitored weekly by its manager or Branch manager, and reviewed monthly by the local Finance department (including average value of cash vs. maximum amount authorized).
- Every cash transaction is monitored, justified, and supported by appropriate documentation.
- Checkbooks, signature plates, cash, and any other means of payment are entrusted only to identified individuals during working hours and secured under lock and key when not in use.
- Cash receipt and cash disbursement operations are segregated from bookkeeping. If Finance management participates in these tasks, an independent monthly challenge (internal or external) is performed.

PC-50-30-140-040

[Risk(s): Authority/limit]

- As mentioned in the Financing, treasury & systems procedures manual, written procedures dedicated to electronic banking define requirements as to documentation, authorized signatures and supervisory approvals. Authorizations are duplicated from checks authorizations.

PC-50-30-140-045

[Risk(s): Misappropriation of assets; Corruption]

- Finance department uses only dematerialized means of payment to pay suppliers. In case of manual operations (transfers, checks…) adequate controls are implemented to mitigate the risks.

PC-50-30-140-050

[Risk(s): Access; Business non-compliance]

- Interface between ERP and Electronic banking system is fully secured at inception, preventing any consultation and/or alteration to payments files while being transferred.
- Secured interfaces through Host to Host services or SWIFT are systematically preferred in order to reduce fraud risk and prohibit manual processing.

PROCESS:

MANAGE TAX

ACTIVITIES

Manage tax activities

PC-50-40-010-010

[Risk(s): Taxation; Financial reporting]

- The preparation of income tax returns is performed in compliance with standards (cut off, interest of the company etc.), regulations applicable to the Group (as CBCR and OECD) and locally, as well as deadlines.
- Corporate income tax returns are properly calculated, paid, reviewed, booked, documented, and validated by management.

PC-50-40-010-020

[Risk(s): Taxation; Financial reporting]

- A review of income tax return is performed regularly by external experts, or at least annually by the external auditors.

PC-50-40-010-021

[Risk(s): Taxation]

- When required, customs duty are calculated according to regulation, documented and validated by management.

PC-50-40-010-022

[Risk(s): Taxation; Financial reporting]

- VAT calculation is documented, justified and validated by management.

PC-50-40-010-023

[Risk(s): Taxation]

- Withholding taxes (if applicable) are properly calculated according to regulation and documented.

PC-50-40-010-050

[Risk(s): Taxation]

- When required, transfer pricings are documented (with market prices and according to Group master file), appropriate documentation is requested (country files) and supervised by the relevant management.

PC-50-40-010-100

[Risk(s): Taxation]

- When required, data related to Country-by-Country Reporting (CbCR) and the Global Anti-Base Erosion (GloBE) Minimum Tax (including the designation of the Ultimate Parent Entity) is disclosed according to the Group's CbCR and GloBE procedures and data file. Relevant information is requested from HQ, and the filings are overseen by the appropriate management.

ACTIVITIES

Manage tax risk

PC-50-40-020-010

[Risk(s): Taxation]

- ▶ Every year, each OPCO completes the Tax questionnaire to be sent to the Group Tax Department.
- ▶ The tax questionnaire includes different information. Specifically, any topic/ issue on transfer pricing systematically receives prior clearing from Group SVP Tax, who is also, conjointly with local management, associated in the action/decision process.
- ▶ In case of Tax audits, at the notification reception before the tax audit opening, each OPCO must notifies Group SVP Tax.

PROCESS:

MONITOR SHARED SERVICE CENTER

ACTIVITIES

Monitor shared service center

PC-50-60-010-010

[Risk(s): Performance measurement]

- ▶ There is a formal SLA to list and agree on the services to be provided by the SSC.
- ▶ KPI are implemented to monitor the SSC's performance.
- ▶ There is a process to ensure that OPCOs financial information is timely and in a suitable way delivered to Sonepar finance department for presentation and submission before Sonepar Board.

PROCESS:

MANAGE TRAVEL EXPENSES

ACTIVITIES

Define and maintain a travel policy

PC-50-70-010-010

[Risk(s): Misappropriation of assets; Authority/limit]

- ▶ There is a valid written Travel and Expense (T&E) policy, aligned with the Group T&E guidelines, reviewed annually and communicated to all associates. It includes:
  - authorization levels;
  - recommended amount of spending for food;
  - class booking for flights;
  - hotel category;
  - cash advances authorization cases (and approval + accounting method);
  - authorized nature of expenses - according to Group guidelines;
  - safety and security measures (incl. insurance coverage and authorization process when travelling to high risk countries) and group travel restrictions.
- ▶ A formal approval is given by management to clear authorization for travel purposes. A travel request form is issued before initiating travel arrangements.
- ▶ Authorization granted to associates to approve travel are in line with internal delegation of authority.

PC-50-70-010-020

[Risk(s): Performance gap]

- ▶ There is an agreement with a preferred partner at least for airfare, car rental, hotel at OPCO or country level. The split of expenses booked by the travel agency or directly by the associate is clearly defined.

ACTIVITIES

Manage and monitor corporate credit cards

PC-50-70-015-010

[Risk(s): Misappropriation of assets]

- ► A formalized local Corporate Credit Card Policy is established, communicated, and periodically reviewed.
- ► The policy defines, at a minimum:
  - eligibility criteria for cardholders;
  - the request and approval workflow;
  - authorized corporate card types;
  - credit limits, terms, and conditions of use;
  - monthly statement reconciliation requirements;
  - cardholder responsibilities;
  - management oversight responsibilities;
  - consequences for non conformance.
- ► Ongoing monitoring activities are performed to ensure continued compliance with the Corporate Credit Card Policy. These activities include:
  - periodic validation of active and terminated associates;
  - confirmation of card activation status;
  - review of card assignments and usage to detect anomalies or inappropriate access.

PC-50-70-015-020

[Risk(s): Misappropriation of assets]

- ► Where permitted by local legislation, corporate credit cards are configured to settle through the associate's personal account to reinforce individual accountability for timely reconciliation and proper documentation.
- ► When corporate cards are settled from the company's bank account, timely submission and reconciliation are reinforced through documented monitoring and escalation procedures to ensure that all transactions are reviewed, supported, and approved without delay.

ACTIVITIES

Monitor the travel and entertainment expenses reimbursement process

PC-50-70-020-015

[Risk(s): Misappropriation of assets; Corruption]

- ► All expenses reimbursement must indicate at least:
  - business purpose;
  - original proof of purchase (credit card statements are not a valid proof of purchase);
  - detail of the beneficiary/ ies.
- ► T&E expenses claims must be submitted at least once a month.
- ► T&E expenses are approved at M+1 level (minimum) even when not on the same site (approval by electronic signature or email).
- ► The business purpose and compliance with the local T&E policy are the approver's responsibility and must be validated prior to authorizing Payment.

PC-50-70-020-020

[Risk(s): Accounting information; Misappropriation of assets; Corruption]

- ► An analytical review of the expense accounts is performed, at least annually, by business / financial controller.
- ► An analytical review of the expense report is performed by a financial / business controller (to provide a review of what is being booked in accounting).

PROCESS:

MONITOR USER ACCESS

ACTIVITIES

Monitor user access

PC-50-80-010-010

[Risk(s): Access; Authority/limit]

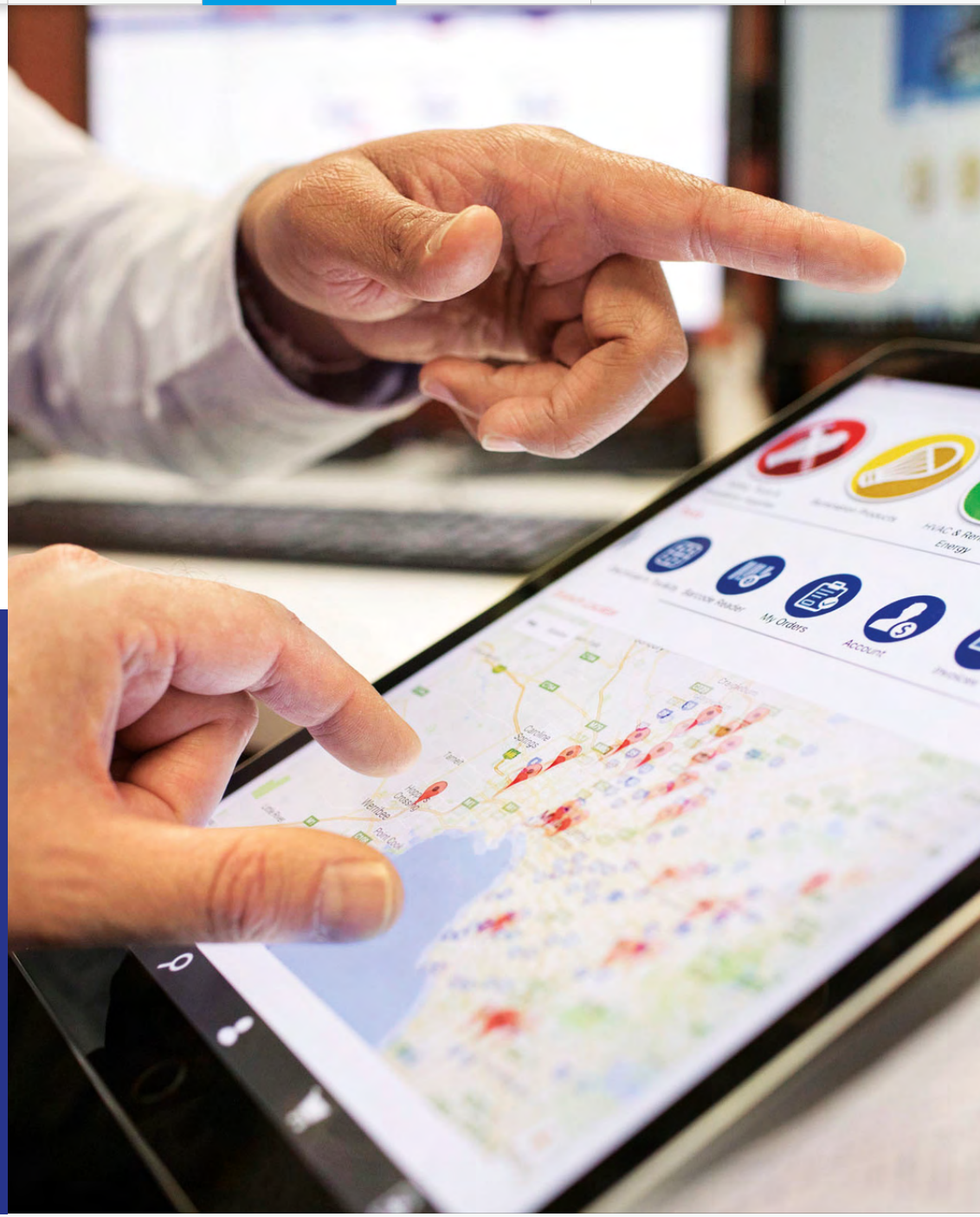
- Managers ensure that proper segregation of duties is in place (e.g. cash receipts/disbursements duties are segregated from those of book-keeping) and regular access reviews are performed (at least on a yearly basis). User access to sensitive transactions and systems (manual entries, payroll data in budget process, treasury tools...) are secured and monitored.
- Exceptions to the segregation of duties principles must be properly documented and mitigating controls in place.

PC-50-80-010-020

[Risk(s): Accounting information; Corruption]

- System prevents users from modifying any data after an accounting period has been closed.

Information & Technology



PROCESS:

PLAN AND ORGANIZE

ACTIVITIES

Define a strategic IT plan

PC-60-10-010-010

[Risk(s): IT infrastructure; Innovation; IS lifecycle management]

- ► IT / ICT plan is prepared by IT Department and reviewed annually by the Board.
- ► IT / ICT plan includes:
  - an assessment of present and future business users' needs, to achieve the company's midterm objectives;
  - software projects and hardware enhancements or replacements to be forecast in the next 2 to 3 years;
  - an assessment of software editor's / provider company's sustainability.

ACTIVITIES

Ensure availability of IT resources

PC-60-10-030-010

[Risk(s): IT infrastructure]

- ► IT architecture is described and responsibilities are defined in accordance with the Board instructions/decisions.
- ► IT architecture is reviewed annually by the Board.
- ► IT architecture is scaled in order to ensure that systems and solutions are able to answer to all needs, requests and exposures and could adapt to changes in scalability, especially in anticipation of SparK roll-out.

PC-60-10-030-020

[Risk(s): Transformation]

- ► User training is included in project management: training needs are identified, a specific budget is attached to training programs, and up-to-date user manuals are available.

PC-60-10-030-040

[Risk(s): Performance gap; IT infrastructure]

- ► Help desk activities are established following a procedure validated by IT Department.
- ► Specifically, they ensure that all queries are logged and tracked until completion.

PC-60-10-030-050

[Risk(s): Performance gap; IT infrastructure]

- ► The Service Desk Manager (or equivalent) regularly reviews service level (according to a defined policy), investigates deviations from service level thresholds, and explains and documents the results in the review documentation.
- ► Appropriate correction / evolution is implemented if needed.

ACTIVITIES

Manage physical security

PC-60-10-040-010

[Risk(s): Access; IT asset damage; Cybersecurity]

- ► The definition and selection of the physical sites for IT equipment is in line with IT and overall business strategy.
- ► The selection and design of the layout of a site takes into account the risk associated with natural and man-made disasters, while considering relevant laws and regulations, such as occupational health and safety regulations.
- ► Access to the server room is appropriately secured and limited to authorized personnel only. Accesses are registered & monitored on a regular basis by the appropriate person.

ACTIVITIES

Manage project

PC-60-10-050-010

[Risk(s): Transformation; Cybersecurity]

- ► IT projects are monitored and formalized. Needs and CyberSecurity risks must be properly defined (scorecard, legal impact, business needs…) and

prioritized. CyberSecurity risks must be studied, assessed and documented during the entire lifecycle of the project.

- ► Regular committees must be held before, during and after completion of the project (prioritization, architecture, costs, answer to business needs, CyberSecurity risks coverage etc.).

PC-60-10-050-020

[Risk(s): Budget & planning; IT infrastructure]

- ► Regular testing occur (non regression, incidents...). Releases must be reviewed and validated. IT environments (development, testing and production) are separated.

PROCESS:

BUILD, ACQUIRE AND IMPLEMENT

ACTIVITIES

Manage changes

PC-60-20-030-010

[Risk(s): Transformation; IS lifecycle management; IT infrastructure]

- ► There is a procedure in case of changes to applications, systems, network, etc. This procedure is applicable even if changes are externalized (e.g. development externalized, configuration change made by a 3rd party, etc.).
- ► This procedure covers:
  - the process to follow in case of request for application changes or new development;
  - assessment of IT and business impacts and risks;
  - stakes, roles and responsibilities in the testing and production environments.
- ► ICT application changes are prioritized before submission to the ICT Committee which makes the final decision in compliance with the applicable "Sonepar's ICT organization".

ACTIVITIES

Manage the datalake

PC-60-20-040-010

[Risk(s): Data integrity; IT infrastructure]

- ► Quality of row data used in the Datalake and for MDM (Master Data Management) is ensured, according to Group guidelines and in line with the common language defined in coordination with HQ. If necessary, action plans for data quality improvement are defined with the country manager and validated with HQ.

PROCESS:

DELIVER SERVICE AND SUPPORT

ACTIVITIES

Ensure continuity of systems

PC-60-30-010-010

[Risk(s): IT asset damage; Crisis management; Cybersecurity]

- ► A Disaster Recovery Plan has been prepared by IT Department, approved by the appropriate level of management and tested; it sets rules of conduct for different levels of system disruptions, up to a major or total breakdown. This plan includes procedures for restoring systems, providing new equipment in case of loss of the IT infrastructure (e.g. following a natural disaster or a cyber-attack) and is designed to describe and to assign tasks to be performed by the IT team members and the system's users in such cases, until return to normal situation. It is built on the concepts of RTO (Return Time Objective: the targeted duration of time and a service level within which a business process must be restored after a disaster) and RPO (Recovery Point Objective: the maximum targeted period in which

data might be lost from an IT service).

- ► Specific topics such as automated scanning (and mitigating solutions in case of malfunction) and other automated warehouse elements must be included.
- ► IT related parts of the Business continuity plan and at least the DRP are reviewed annually by IT Department (or more often in case of change(s) in the tool during releases that may impact the relevance of tests).

PC-60-30-010-015

[Risk(s): Cybersecurity]

- ► The appropriateness, effectiveness and efficiency of DRP is checked in tests and exercises, according to the criticality of the system and at least annually. Results of these tests and exercises are kept to allow historical analysis.

PC-60-30-010-020

[Risk(s): Crisis management; IT asset damage]

- ► A crisis management model is defined, based on a single team dealing with operational and decisional aspects or split in two dedicated taskforce teams. The model:
  - identifies & defines crisis stakeholders, roles and responsibilities;
  - formalizes crisis management documents repository: crisis directory...;
  - if applicable: is in capacity to conduct a local crisis exercise, i.e. providing feedback improving crisis management process.

ACTIVITIES

Perform backup

PC-60-30-040-010

[Risk(s): Cybersecurity; IT asset damage; Crisis management]

- ► All the production servers are backed up, restoration processes are defined and tested at least once a year. These tests are reviewed, traced and signed by management annually. When possible backup infrastructure is segregated.
- ► All production servers handling critical data (either on premises or in the Cloud) are automatically backed up on two different storages, one of them being offline (without direct access to the production system). Restoration and failovers are reviewed at least annually and traced to ensure the process is operational.

ACTIVITIES

Ensure integrity of IT and system security

PC-60-30-050-010

[Risk(s): Cybersecurity]

- ► The set of Group Cybersecurity Policies is communicated and applied locally. Adaptations, exceptions and derogations to Group CyberSecurity Policies are traced.

PC-60-30-050-011

[Risk(s): Cybersecurity; Crisis management]

- ► There is a business risk analysis, including identification, mapping and evaluation of cyber risks with an annual review for critical risks. There is an IT roadmap established yearly.

PC-60-30-050-012

[Risk(s): Cybersecurity; IT asset damage; IT infrastructure]

- ► Each company ensures that:
  - New perimeter are onboarded within vulnerability scans and declared in Vulnerability Management portal,
  - All systems are scanned and declared in Vulnerability Management portal.
- ► Once a vulnerability has been identified, an action plan is defined in order to correct the vulnerability in a due time according to its criticality and in compliance with timeline defined by Group CyberSecurity team.

PC-60-30-050-013

[Risk(s): Access; IT infrastructure; Cybersecurity]

- ► Manage EDR solution (Devices protection).
  Each OPCO:
  - Is in capacity to respond to threat attack, focused on Workstations and Servers behaviors (Windows, Linux, MAC OS);
  - Deploys the solution by default on all new endpoints provisioned by IT (included in OS Master);
  - Deploys the solution on all technically compatible workstations and servers;
  - Defines and maintains enrollment of EDR sensors lifecycle operational procedure (deploy, update, deinstallation, deregistration, versions, additional settings recommendations) provided by Group Cyber Team.

PC-60-30-050-015

[Risk(s): IT asset damage; IT infrastructure; Performance gap]

► There is a regular performance analysis including:
- performance of application and databases integrity tests;
- relevant controls over applications or transactions that are executed /processed by external service providers;
- logging of all systems disruptions and failures.

PC-60-30-050-018

[Risk(s): Cybersecurity]

► Security awareness is deployed within the organization by performing at least 1 awareness campaign per year (social engineering, phishing, authentication, data handling, unintentional data exposure, security incidents…), targeting all people, including external contractors.
► New users, whether internal or external, must receive cybersecurity awareness content as part of their onboarding procedure.

PC-60-30-050-019

[Risk(s): Cybersecurity; Access]

► Email flow is protected:
- For Inputs Email traffic (external -> Sonepar): by securing SMTP flows; checking that all associated SMTP MX domain records are managed.
- For Outputs Emails traffic (Sonepar -> Internet): by securing outputs traffic; checking that all outputs mail flow are going through protection platform.

► Email Flow is authenticated:
- All domains (sending and non-sending emails) must have a DMARC policy hardened to "p=reject";
- All domains (sending and non-sending emails) must have a SPF record.

PC-60-30-050-020

[Risk(s): Cybersecurity; Access]

► In order to review and manage local computer password:
- LAPS is deployed on domain joined servers and GPO (Group Policy Object) is configured to enforce local account password renewal.
- Password renewal issues are reviewed and fixed (and escalated to Group support team if needed).
- Password must respect the Group Password Policy and must be specific to each application account.

PC-60-30-050-022

[Risk(s): IT infrastructure; Capacity]

► All subscriptions to Azure cloud are done on the Sonepar Group contract (mono tenant solution) and local contracts are forbidden.

PC-60-30-050-023

[Risk(s): Cybersecurity; Data protection]

► According to IT data classification guidelines, the following items are properly defined:
- a data classification based on criticality;
- the roles, responsibilities, owners and custodians of the various types of information;
- the retention time (in accordance with applicable laws and in line with personal data retention principles and requirements);
- the process for handling and protecting data, i.e. the general/default security controls and methods of use according to the classification;
- the classification of information backups.

PC-60-30-050-024

[Risk(s): Access]

► To protect access to applications:
- Password must respect the Group Password Policy and must be dedicated for each use;
- Multi-Factor Authentication must be enabled for all applications exposed to the whole Internet.

PC-60-30-050-030

[Risk(s): IS lifecycle management]

► Licenses are up to date and paid for and a complete inventory is made and maintained by IT Department. Coherence with other market solutions and decommissioning is followed and monitored.

PC-60-30-050-040

[Risk(s): IS lifecycle management]

► There is a yearly review of IT assets' obsolescence with the formalization of a lifecycle roadmap. It includes the existence of maintenance contracts, the analysis of the possibility or not to continue patching, and the definition of the mitigation controls in place in case no patching is possible.

PC-60-30-050-050

[Risk(s): Cybersecurity]

- As part of Cybersecurity detection & response activity, all CyberSecurity systems (DNS, DHCP, Firewalls, Web Proxy, IPS/IDS, Remote Access (VPN)…), infrastructures (Active Directory…), and critical application servers are onboarded into Group CyberSOC. List of scope to be onboarded is provided by GroupCyberSOC.
- List of monitored assets are updated when new asset is added, changed or removed. New or discovered assets are integrated into the CyberSOC.

PC-60-30-050-060

[Risk(s): Cybersecurity; Crisis Management]

- As part of Cybersecurity detection & response activity, local security incident process and procedure are documented and are aligned with the Global Security Incident Management Process. This ensures that security incidents are managed by local teams in collaboration with the Group's CyberSOC to deal with detected incidents.

PC-60-30-050-070

[Risk(s): Access; Cybersecurity; IT infrastructure]

- Network segregation must be documented (network diagram) and enforced using Group CyberSecurity solutions to separate the following perimeter:
  - User perimeter (Workstations) vs. Resource perimeter (servers in datacenters);
  - Non-production vs. production environments;
  - Industrial vs. office networks.

PC-60-30-050-080

[Risk(s): Access; Cybersecurity]

- Hard disk of all laptops must be encrypted.

PC-60-30-050-085

[Risk(s): Data protection; Cybersecurity; Access]

- Sensitive data transiting on systems and networks on which Sonepar is not authoritative must be encrypted at rest and in transit. Encryption protocols and encryption keys must comply with the best practices defined in the Cybersecurity reference documents.

ACTIVITIES

Manage user access / Monitor super-user profile

PC-60-30-070-010

[Risk(s): Access; Authority/limit; Cybersecurity]

- According to a local procedure, all requests for creations in user access (for applications and transactions) are formally documented and approved by the appropriate level of management. Generic accounts are not approved or created. Segregation of duties are taken into account in the creation process.
- Principle of least privileges is applied (the user only have access to the resources and data needed).
- The provision of rights must be based on the RBAC (Role Based Access Control) model.
- Access of terminated users is disabled and changing profiles are updated based on timely communication of the HR Department.
- User identities accessing Sonepar's authoritative systems must be managed during their entire lifecycle (Joiner, Mover and Leaver).

PC-60-30-070-030

[Risk(s): Access; Cybersecurity]

- An automatic IT control is in place to make sure unused / inactive screens / sessions are automatically logged out.

PC-60-30-070-035

[Risk(s): Cybersecurity]

- To guarantee a secure working environment, ensure that:
  - Each OPCO has a patch management process defined locally;
  - All computers are rebooted every week;
  - All servers are rebooted every month.

PC-60-30-070-060

[Risk(s): Access; Authority/limit; Cybersecurity]

- Privileged accounts (super-users) are limited to IT administrator accounts (dedicated to the administration of PCs, Servers, Active Directory…
- Those accounts are different than standard user accounts used for day-to-day activities (e.g., reading emails…).

- The provision of rights must be based on the RBAC model;
- Principle of least privileges is applied on those accounts (only required permissions are granted to the privileged accounts);
- Multi-Factor Authentication must be enabled for all IT administrator accesses.

► An annual review of privileged accounts is performed.

ACTIVITIES

Control assets and applications inventory

PC-60-30-090-010

[Risk(s): IS lifecycle management; IT infrastructure; Misappropriation of assets]

► There is a full inventory of the IT assets and applications (physical, hardware and software on which Sonepar is authoritative). It is updated at each step of asset lifecycle (new asset, decommissioning...). Criticality of each asset that would be used as part of a rebuild / restart plan after a potential cyber incident is defined. Inventory counts of IT assets are performed on a regular basis (defined at local level) and a global review is performed at least on an annual basis. Asset adjustments are investigated and authorized by appropriate management. Individuals who can maintain master data do not have access to the IT assets' stocks.

Asset on which Sonepar is authoritative : IT asset on which Sonepar can decide what to do (decision-maker even if not direct owner).

Human Resources

PROCESS:

MANAGE PEOPLE (PLANNING, RECRUITMENT, TERMINATION)

ACTIVITIES

Hire new employees and manage terminations

PC-70-10-010-010

[Risk(s): Skills and knowledge capital; People departure]

► According to local procedures, recruitments and terminations are subject to prior approval by appropriate level (according to Sonepar principles / Grandfathering) based on:
- a job description stating the needs for recruitment validated by relevant department manager;
- a consideration of annual wage budget;
- a termination form stating associate name, termination date, reason for termination and balance of account approved by relevant department manager.

PC-70-10-010-020

[Risk(s): Labor laws]

► Employment contract and amendment templates are periodically reviewed to ensure compliance with relevant labor laws and social regulations, and are signed by the appropriate level of management to ensure the "4-eye principle."

► Employment contracts and amendments to contracts of country/OPCO key associates are approved by the country/OPCO board of directors as required.

PC-70-10-010-025

[Risk(s): Succession Planning; Skills and knowledge capital]

► The risk of having only one (internal or external) knowledgeable person for sensitive/key processes or systems is either low or mitigated to an acceptable level by appropriate actions, for example by:
- tagging in Sonepeople the “key positions” (by HR);
- choosing in the Sonepeople talent search the “Departure risk level” and “Business Impact of Departure” of associates (by Manager);
- including in the Sonepeople succession plan and talent reviews, the analysis of these previous criteria's for the concerned associates;
- flagging an « emergency plan » in the succession plan proposals (associates able to be immediate back ups);
- formalizing in the job descriptions, main associated procedures and back up possibilities of concerned associates.

PC-70-10-010-030

[Risk(s): Data integrity; Data privacy]

► New hire information is recorded by HR Department based on a checklist to ensure accuracy and completeness (incl. administrative and banking information).

PC-70-10-010-035

[Risk(s): Skills and knowledge capital; Performance gap]

► For final selected candidates (management positions and above), reference checks are systematically authorized by the proper level of management, performed and documented.

PC-70-10-010-050

[Risk(s): Performance measurement]

► Every month, HR Department supervises headcount reporting, including reports documenting new hires and terminations. Reports are validated by HR department.

► There is a monthly communication of reports to the IT department in order to align respective headcounts reports and update the IT system accesses.

PC-70-10-010-065

[Risk(s): Performance gap; People departure]

► There is an onboarding documented procedure.

PC-70-10-010-070

[Risk(s): Access; Misappropriation of assets]

► There is a documented exit procedure. When an associate leaves the company, there is a procedure to ensure that badges and keys, along with all accesses granted (physical and to IT systems) are canceled/returned.

ACTIVITIES

Follow and analyze HR KPIs

PC-70-10-020-010

[Risk(s): Misappropriation of assets; Health and safety; Inclusion]

- ▶ Group HR KPI's are published and communicated according to the frequency determined at Group level:
  - Headcounts, gender split, average age, average seniority, attrition rate, attrition rate < 3 years, resignation rate (voluntary departure), sickness ratio, Hirings % Women, Internal mobility and internal mobility % Women are reported quarterly to the group. A consolidated version is communicated yearly via the strategic IMPACT plan.
  - Staff costs, contribution per FTE, sickness KPIs are provided by controlling team to HR Group quarterly.
  - Attrition rate and below 3 years seniority attrition rate (for countries included in the Impact Plan) are reported yearly to the Group.
- ▶ HR indicators are implemented, followed, analyzed and communicated to all relevant personnel to allow pro-activity and full involvement of personnel to company's objectives.

PC-70-10-020-020

[Risk(s): Inclusion; Talent attraction; Corporate culture]

- ▶ Inclusion Key Performance Indicators (KPIs) are evaluated at the country level and reported to the Group on an annual basis. They include:
  - Gender split;
  - Inclusivity ("Our recruitment and career advancement processes are transparent, objective, and ensure equal opportunity for all" from last Open Voices' survey);
  - Gender split in succession plans;
  - Percentage of associates trained on Inclusion;
  - Percentage of associates with a position in the 9-box grid;
  - Percentage of associates with disabilities (when legally possible);
  - Percentage of Inclusion index from Open Voices.

PROCESS:

MANAGE PEOPLE'S PERFORMANCE AND DEVELOPMENT

ACTIVITIES

Evaluate employees

PC-70-20-010-010

[Risk(s): Skills and knowledge capital; Performance gap]

- ▶ Evaluation of associates is based on predefined criteria and regularly performed through:
  - annual performance assessment interviews;
  - objective setting and evaluation;
  - incentive schemes.

ACTIVITIES

Develop succession and career plans

PC-70-20-020-010

[Risk(s): Succession Planning]

- ▶ Country/OPCO key associates' succession plan are validated by the country board or above according to the Group's approval matrix. SLP (Sonepar Leadership Program) and SJC (Sonepar Junior Committee) members have formalized development plans.

PC-70-20-020-030

[Risk(s): Skills and knowledge capital; Performance gap]

- ▶ Every associate completes his/her performance review in Sonepeople by March of each year (incl. systematically leadership competencies for executives).
- ▶ Every manager completes the talent review for their team members in Sonepeople by August of each year.

ACTIVITIES

Develop and train employees

PC-70-20-030-010

[Risk(s): Skills and knowledge capital; Performance gap]

► A multiannual training offer is established by HR department, reviewed by the relevant management, with definition of key themes to reach the aims of the organization.

PC-70-20-030-020

[Risk(s): Skills and knowledge capital; Performance gap]

► All associates are required to complete in Sonepeople mandatory trainings as mandated by the Group, such as Compliance, Cybersecurity, Inclusion, Sustainability, Health & Safety as well as any additional trainings required by local laws and regulations.

► In addition, an individual training program is validated by Human Resources Department, in collaboration with the associate's manager who:

- communicates training opportunities to associates at least annually;
- takes into consideration applications for training;
- monitors training budget;
- evaluates the relevance of training programs.

ACTIVITIES

Maintain objectives & strategic alignment

PC-70-20-040-020

[Risk(s): Performance gap]

► Individual objectives are assigned to executives in the company and then cascaded to branch and operational users.

► The bonus and incentive rules are defined and consistent with goals and objectives. For executives, bonuses are aligned with the Group standards in terms of size and structure.

PROCESS:

ENSURE COMPLIANCE WITH LABOR REGULATIONS

ACTIVITIES

Ensure compliance with labor regulations

PC-70-30-010-010

[Risk(s): Pension funds; Accounting information]

► All pension plans are updated and revalued, at least at company's Group consolidation closing dates, to ensure accurate valuation of company's liabilities. Any revaluation uses IFRS standards.

PC-70-30-010-015

[Risk(s): Pension funds; Authority/limit]

► No pension plan for country key associates can be implemented without Sonepar President and/or Chief People & Engagement Officer prior approval, according the Group's approval matrix.

PC-70-30-010-020

[Risk(s): Labor laws]

► Overtime for associates must comply with the law.

PROCESS:

MANAGE PAYROLL

ACTIVITIES

Determine and approve wage plan

PC-70-40-010-010

[Risk(s): Performance gap; Authority/limit]

- Annual wage plan and the relevance of variable wage's policy are evaluated by HR department, reviewed/commented/validated by the relevant management.
- The company salary increases as well as the individual ones are communicated and validated annually by the relevant management. Key executives' increases and bonuses are approved by Sonepar President and/or Chief People & Engagement Officer as provided by the Group's approval matrix. HR department supervises the process and results.

ACTIVITIES

Review payroll processing and other payments to management and employees (excl T&E)

PC-70-40-040-020

[Risk(s): Data integrity; Authority/limit]

- Any modification of associate's remuneration and/or position is supported by an approved official document in line with internal validation of authorities.

PC-70-40-040-040

[Risk(s): Access; Authority/limit; Data integrity]

- There is a formalized procedure for creation and modification of associates' data.
- Individuals allowed to make entries containing associates' data in IT systems are limited by user access setups in those systems.
- This information is entered into the system in a timely manner and reviewed by an individual without access to database modifications.
- In case of bank information modification, a verbal confirmation by the associate is required.
- Access to all information regarding associates is restricted.

PC-70-40-040-050

[Risk(s): Authority/limit; Data integrity; Accounting information]

- As formalized in a procedure, payroll is prepared by payroll manager in accordance with labor regulations and independently reviewed by the relevant HR manager ("4 eye principle").
- Each payment made to an associate has to be supported by a valid and relevant documentation (employment contract, bonus agreement, terms of employment, and final settlement).
- Accesses to payroll system are granted to a limited number of individuals who strictly need to have access to process the payroll, in compliance with the principle of segregation of duties.
- Monthly final payment proposal is reviewed by the relevant HR manager and signed by finance manager before being processed by the bank.

PC-70-40-040-100

[Risk(s): Data protection]

- In case of outsourced payroll services, the data transfer, processing and returning of information is formalized in a contract signed with the external company based on a service level agreement that will be incorporated in a dedicated internal procedure.

PC-70-40-040-130

[Risk(s): Misappropriation of assets]

- Deposit and advances are strictly followed-up by HR department who will allow their process when calculating the net salary to be paid.
- Duly approved supporting documents are centralized within HR department.

PC-70-40-040-140

[Risk(s): Taxation; Labor laws]

- Social Regulations (eg: fringe benefits, benefits in kind…) are taken into account in the income tax return computation.

ACTIVITIES

Ensure accuracy of payroll journal entries

PC-70-40-050-010

[Risk(s): Accounting information]

► Accruals for salaries (vacation benefits, holidays…) are prepared, reviewed and approved by management.

PC-70-40-050-030

[Risk(s): Accounting information]

► All defined benefits plans to associates and management are identified and accounted for in financial reporting.

PC-70-40-050-040

[Risk(s): Pension funds; Accounting information]

► If applicable, there is a regular review and analysis of pension liabilities and compliance with IFRS standards.

NEW PC-70-40-050-050

[Risk(s): Data integrity]

► There is a formalized reconciliation between the associates masterdata and the data in the payroll system (headcount, bank information…).

PROCESS:

MONITOR HR ACTIVITIES

ACTIVITIES

Monitor user access

PC-70-60-010-010

[Risk(s): Access; Authority/limit]

► Managers are in charge of ensuring that proper segregation of duties is in place (especially payment and general ledger entry duties) and regular IT access reviews and controls are performed (e.g. Sonepeople accesses, incl. those temporarily allocated).

ACTIVITIES

Follow satisfaction survey

PC-70-60-020-010

[Risk(s): People departure]

► Group satisfaction survey (IPSOS) is deployed locally by each country. Additionally, local surveys can be launched according to local stakes.

ACTIVITIES

Ensure data quality

PC-70-60-030-010

[Risk(s): Data integrity]

► The data quality available in Sonepeople is ensured to be up to date, reliable, complete for reporting and analysis purposes, by the HR leader in coordination with the responsible data controller.

Governance, Risk & Compliance

PROCESS:

ENSURE COMPLIANCE WITH CORPORATE STANDARDS

Sonepar has the responsibility, as a global company, to ensure that its activities are always in line with the highest ethical standards in every country in which the Group operates.

To that end, several documents have been formalized:

- The Code of conduct: It is the reference document for global compliance and integrity within Sonepar, that sets out the principles and rules of good conduct that must guide all Sonepar's associates in their daily business, everywhere and every day.
- The Business Partners code of conduct: Sonepar expects its business partners to commit to a high level of ethics. As such, specific standards are set out in a dedicated Business Partners Code of Conduct and the Group has deployed procedures and tools to assess the integrity of its business partners.
- The Compliance Manual: In order to effectively implement the principles and standards set out in Sonepar's Code of Conduct, various topics are dealt with more specifically in this document, such as promoting fair competition, preventing corruption, protecting data privacy, or complying with embargoes and international trade regulations.
- The Speak Up Policy provides a way for those who are aware of circumstances or behaviors which they believe, in good faith, could represent violations of Sonepar's Code of Conduct, Business Partners Code of Conduct, Policies and Procedures and/or applicable laws and regulations to identify and share those concerns.

ACTIVITIES

Develop corporate governance

PC-80-10-010-010

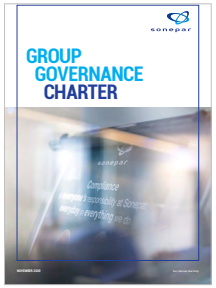
[Risk(s): Business non-compliance; Corruption; Anti-competitive practice]

- ▶ Each OPCO ensures that the Code of Conduct and the Compliance Manual (including inter-alia the anti-corruption policy and the speak up policy) are available to all their associates and newcomers and published on local intranets. New compliance posters are being permanently displayed in all HQs, offices, sales points and CDCs .
- ▶ The Group Code of Conduct and the Business Partners Code of Conduct are made available to Sonepar's business partners on local websites and implemented, as appropriate, in the contractual documentation or separately.

PC-80-10-010-020

[Risk(s): Business non-compliance]

- ▶ The Group Governance Charter is communicated at appropriate level.



The aim of the Sonepar Governance Charter is to:

- Set forth the founding values and philosophy that guide the way the Group is operated and inspire the day-to-day behavior of its members
- Describe and implement common references and governance documents within Sonepar's decentralized organizational structure that comply with the principle of subsidiarity, i.e. clear responsibilities established at the most relevant levels with no gaps or overlaps.

This Charter covers two forms of governance: corporate governance and operational governance.

PC-80-10-010-040

[Risk(s): Corruption; Business non-compliance]

► Any potential personal involvement in a business investment or operation outside the Group, which could determine a conflict of interest, is disclosed by associates at proper level as per Sonepars' Conflict of Interest Policy.

PC-80-10-010-050

[Risk(s): Authority/limit]

► The latest updated Group Approval Matrix is adapted (with local thresholds), implemented at local level, and translated if necessary. The Local Approval Matrix is made available to all associates and newcomers, and published on local intranets where applicable.

The Group Approval Matrix is a key document to secure sound governance and risk management across Sonepar.

The Group Approval Matrix covers a wide range of business topics such as acquisitions, capital expenditures, customer and supplier contracts, but also addresses the required approvals for the Finance, Legal, Digital Enterprise, Human Resources and Communication Departments. It is available on the Group intranet.

PC-80-10-010-060

[Risk(s): Executive management]

► Board / Executive committees exist for each managerial area. These governing bodies provide oversight for management's activities.

PC-80-10-010-070

[Risk(s): Transformation; Business model]

► As part of the Digital Enterprise Transformation, through the Impact Plan presentation, each OPCO reviews and defines:
- its maturity assessment of Business capabilities;
- its digital Enterprise roadmap (based upon the maturity assessment and the defined strategy on the 5 digital axes: value proposition by customer, omni-channel go-to-market position, supplier & customer ecosystem innovation, operational productivity and data as a strategic asset);
- its associated Investments to the Digital Enterprise Roadmap.

ACTIVITIES

Prevent and report fraud and abuse

PC-80-10-020-010

[Risk(s): Business non-compliance; Corruption; Anti-competitive practice]

► The Group Code of Conduct and the Compliance Manual contain values and standards applicable within the Group. They are reviewed from time to time. Appropriate trainings and awareness campaign are performed locally on a regular basis in all sites.

PC-80-10-020-030

[Risk(s): Business non-compliance; Corruption; Misappropriation of assets]

► A local process for capturing, reporting, analyzing and escalating all detected fraud, corruption and influence peddling incidents (whatever the amount) is defined and in place.

► In addition, each executive is committed to report all kind of identified fraud, corruption and influence peddling cases to Sonepar HQ according to Group Fraud Reporting Policy and through the Fraud, Corruption and Influence Peddling form (available in Appendix). Local and OPCO Top Management comply with fraud reporting rules defined in the Fraud Corruption and Influence Peddling template.

► All fraud cases are regularly and systematically reported to the Regional President.

► Awareness actions on fraud prevention are organized locally. Fraud prevention cards and IC toolkit are spread (see appendices).

NEW **PC-80-10-020-040**

[Risk(s): Business non-compliance; Corruption; Misappropriation of assets]

► Branch KPIs have been defined and are monitored on a monthly basis as detailed in the "Branch KPIs Dashboard" (see appendices), to control sensitive transactions and identify potential frauds.

PROCESS:

ENSURE LEGAL AND REGULATORY COMPLIANCE

ACTIVITIES

Manage legal and regulatory compliance

PC-80-20-010-010

[Risk(s): Business ethics; Executive management; Corruption]

► Each Regional General Counsel or Country Head of Legal and his/her team is responsible for:
- the proper and efficient handling of all legal affairs of his/her Region (with an emphasis on contracts, M&A, joint ventures, intellectual property and litigation);
- overseeing, supervising and monitoring corporate governance and company law within his/her Region;
- overseeing, supervising, monitoring and assessing compliance with all applicable laws and regulations and with the Group's Code of Conduct and internal policies and procedures (including without limitation business partners assessment);
- providing the necessary guidance and support to his/her Region, including training, for the correct follow up and respect of the Group's Code of Conduct and internal policies and procedures;
- assisting the Regional Presidents in defining and implementing compliance policies and procedures for the Region in accordance with those of the Group, with a view to ensuring that Sonepar's business is carried out diligently, loyally and ethically; and
- assisting the Group General Counsel's Office in investigating suspected violations of applicable laws and regulations, internal rules or procedures and in handling governmental queries and investigations.

► Sonepar General Counsel's Office is being appropriately informed of matters falling under its responsibility such as major M&A deals or litigations, contracting insurance policies.
► Quarterly reporting is sent to the General Counsel.

PC-80-20-010-020

[Risk(s): Authority/limit; Business non-compliance]

► Legal department prepares template agreements as well as guidelines, if and when necessary.
► Legal department reviews material contracts as per the Group and local Approval Matrices.
► Contracts are approved in accordance with the Group and local Approval Matrices and signed by duly authorized representatives of the legal entity.

PC-80-20-010-025

[Risk(s): Business non-compliance; Third-party non-compliance]

► General Terms of Sales are implemented with the help of the legal department and approved by local top management. They are updated from time to time as necessary to reflect changes in Sonepar policies and procedures or changes in applicable laws and regulations.

PC-80-20-010-030

[Risk(s): Third-party non-compliance; Corruption]

► An assessment of capabilities and quality of third-party services (especially concerning: Legal, Payroll, Safety), as well as a review of third-party compliance to service agreements are periodically performed by appropriate management.
► Third parties' invoices are challenged.
► Anteriority of third parties is monitored.

PC-80-20-010-040

[Risk(s): Business non-compliance]

- ► Litigation is supervised by Legal Department with the assistance of outside legal counsels if needed.
- ► All litigations above 100k€ have to be reported and monitored in the Group tool Dilitrust.
- ► Provisions or settlements concerning claims and litigations (including without limitation tax disputes) are approved in accordance with the Group and local Approval Matrices.

PC-80-20-010-050

[Risk(s): Data privacy]

- ► Record retention / archiving procedures comply with applicable regulations and meet the company's needs and requirements.
- ► Specifically, Company legal documents are suitably preserved.

PC-80-20-010-060

[Risk(s): Business non-compliance; Corruption]

- ► Twice a year, in December and June, sales made with deliveries in countries where Sonepar does not have any legal entity are reported to the Group General Counsel. If a specific license is required to sell the products in said countries, the license must be attached to the turnover declaration provided to the Group General Counsel.

ACTIVITIES

Manage the offering and receiving of gifts and gratuities

PC-80-20-020-010

[Risk(s): Corruption; Business non-compliance]

- ► The Gifts, Invitations and Travel-related expenses Policy available in the Compliance Manual is applied.
- ► The required Regional Policy has been drafted, approved, implemented and communicated to all associates in the Region in accordance with the Compliance Manual. It shall include:
  - the applicable regional approval thresholds;
  - the monitoring process;
  - potential additional and more restrictive guidelines than the ones set in the Compliance Manual;
  - the process to distribute left-over gifts linked to promotional campaigns; and
  - local practical examples.

PC-80-20-020-020

[Risk(s): Corruption; Business non-compliance]

- ► A declaration including the list of gifts offered to customers is submitted to the relevant organization.
- ► A process is implemented in order to gather proof of receipt by the customer.

PC-80-20-020-030

[Risk(s): Corruption; Business non-compliance]

- ► Gifts, Invitations and Travel-related expenses are followed-up by individual and category, as per the Regional Policy.
- ► A formal approval is given by management to clear authorization for gift and entertainment purposes before the expense is incurred.
- ► Authorization granted to associates to approve gifts and entertainment are consistent with internal delegation of authority.
- ► Customers' gifts are monitored every month by someone independent from sales and marketing activities.
- ► The Regional Policy outlines the process for distributing leftover gifts from promotional campaigns, and is overseen by associates independent from sales and marketing activities.
- ► Gifts, gratuities and non-cash compensations offered or received are tracked by beneficiary and category.
- ► Additional rules applying to Gifts, Invitations and Travel-related expenses to Public Officials are strictly followed.
- ► Violations of the Group and/or Regional Policies are reported at appropriate management level.
- ► Approvers and controllers of Gifts, Invitations and Travel-related expenses are designated locally in a matrix communicated to all associates.

PC-80-20-020-050

[Risk(s): Corruption; Business non-compliance]

► Associates receiving gifts from a supplier must declare them to their line manager in accordance with the rules set in the Group and Regional Policies.
► Excess promotional gifts is tracked and returned to suppliers.

PC-80-20-020-060

[Risk(s): Corruption; Business non-compliance]

► Terms & Conditions with suppliers include provisions regarding rules applicable to gifts offered to associates.

ACTIVITIES

Manage data privacy risk

PC-80-20-030-010

[Risk(s): Data privacy]

► **Organization and Governance:**
- The appropriate personal data protection organization and governance has been put in place, so as to identify the various key functions and responsibilities in the local organization in charge of personal data protection;
- Individuals in charge of personal data protection are clearly identified and known to the associates. They have dedicated time allocated for data protection compliance and are given adequate resources and training to fulfill their missions and improve their data privacy knowledge and skills;
- An outside lawyer has been identified to help the local teams address any urgent or high stake situation as regards to data privacy.

PC-80-20-030-011

[Risk(s): Data privacy]

► **Records and mapping:**
- Personal Data processing activities have been identified and documented (e.g., in a dedicated register). They are recorded internally and, as applicable, declared to the relevant data protection authorities. Such records and declarations comply with applicable laws and/or local policies;
- Identification of the Personal Data flows within and outside the organization has been done and/or in construction with the help of the digital transformation teams, at Global or local level;
- Processes are in place to (i) identify any personal data processing subject to the obligation to carry out a privacy impact assessment and (ii) to carry them out, if and when required by applicable law.

PC-80-20-030-012

[Risk(s): Data privacy]

► **Sensitive data:**
- and special categories of data are identified within the organization;
- is processed only if and when required or duly authorized by applicable law;
- receive adequate, and when required, enhanced degree of protection and security.

PC-80-20-030-013

[Risk(s): Data privacy]

► **International transfers of personal data:**
- Transfers of Personal Data outside the country where they are collected:
  - are adequately mapped within the organization;
  - are undertaken in accordance with applicable laws and regulations (such as the European commission Standard Contractual Clauses – SCCs- for transfers outside of the EEA);
  - are subject to prior legal and cybersecurity review as per local processes.

► **EU – US transfers:**
- For EU based processing activities, EU/EEA storage is always preferred.
- Transfers to the US must be made only if no technical equivalent is available or if mandated for the usual activities of the companies at stake and provided such transfers are made in accordance with legal requirements.

PC-80-20-030-014

[Risk(s): Data privacy]

► **Awareness:**
- Associates' awareness has been raised as regards confidentiality and personal data protection. A dedicated training program for associates who process personal data as part of their missions has been deployed.
- The relevant general or specific rules, processes and policies as regards personal data processing activities are available to the associates and/or a deployment plan is being implemented with defined deadlines.

PC-80-20-030-015

[Risk(s): Data privacy]

► **Personal Data Retention:**

- Personal Data are kept only for the duration necessary to accomplish the purpose for which they have been collected or processed. In no event may such duration exceed legally fixed maximum retention periods.
- Appropriate archiving and destruction mechanisms are put in place to sort out and retain only the relevant Personal Data after the appropriate period of retention has lapsed. Archiving is done only when there is a documented necessity (e.g. legal obligation).
- Processes are in place to ensure the same principles are duplicated to services providers that have access to, or host, Personal Data during and at termination of the business relationship.

PC-80-20-030-016

[Risk(s): Data privacy; Cybersecurity]

► **Personal Data Breach:**

A local procedure defines how to handle incidents (cybersecurity breach, internal technical issue, human error, etc.), including the need to have:

- A thorough and immediate evaluation of the impact on personal data undertaken and adequate remediation measures implemented; and
- A legal review immediately performed to assess whether a criminal complaint (French LOPMI law), a notification to the affected data subjects and/or data protection authorities is required within the applicable legal deadlines (in particular 72 hours for GDPR), and adequate measures implemented based on such review.

PC-80-20-030-017

[Risk(s): Data privacy]

► **Data subjects' rights:**

- A local procedure defines how to handle data subjects' requests (right to deletion, to object, to restrict, to data portability, to access, etc.)
- Processes are in place to ensure that technical and organizational measures regarding the data subjects rights are implemented in third parties' tools where Personal Data are processed.

PC-80-20-030-018

[Risk(s): Data privacy]

► **Transparency:**

- Data subjects (associates, candidates, current and potential customers, suppliers, etc.) are informed of the data processing activities undertaken with their personal data as required by applicable laws and regulation. These include any processing undertaken at Group level (such as Sonepeople, Concur, Spark, digital solutions, geographical access and storage, etc.) ;
- Consent to processing has been duly obtained, if and as required by applicable laws.

PC-80-20-030-019

[Risk(s): Data privacy]

► **Processors vetting and management:**

- A data processing agreement or equivalent describing the rights and obligations of the parties as well as instructions from the data controller is signed with data processors, when required by applicable laws;
- Technical and organizational measures of any service provider which processes Personal Data are reviewed and validated in accordance with OPCOs' process and with the help of cybersecurity.

PC-80-20-030-020

[Risk(s): Data privacy]

► **Action Plan and compliance monitoring:**

- An action plan has been established with specific deadlines and milestones to address and remedy gaps in regards to personal data protection and processing principles. It is sent, along with a progress report, to the Group DPO at least once a year.
- Alignment of the compliance with (i) data protection laws and regulations (including, when applicable, the GDPR) and (ii) the personal data protection principles and policies included in Compliance Manual is regularly assessed and monitored.

PROCESS:

ENSURE BUSINESS CONTINUITY

ACTIVITIES

Prepare a business continuity plan and manage employees training and awareness

PC-80-30-010-010

[Risk(s): Crisis management; Performance gap]

► A framework / policy for Business Continuity Management (BCM) is defined and implemented. The BCM policy has been approved and communicated by management and circulated at relevant levels. It is reviewed periodically (at the discretion of Country level Management) and it includes a list of scenarios threatening the achievement of the business objectives (risks and including cyber-risks), risk assessment in terms of likelihood and impact (Business Impact Analysis - BIA), emergency preparedness and response/ resumption of activities in a timely manner as well as progress monitoring.

PC-80-30-010-020

[Risk(s): Crisis management; Performance gap]

► A Business Continuity Plan (BCP) is available and approved in each business location by the appropriate level of management. It is aligned with Group guidelines (when made available) and includes the following:
- Definition of organizational (including work organization, remote work…) and technical modalities to ensure a fast and effective response, work in a degraded mode and gradual resumption of its activities;
- The BCP resource team members and their contact information
- Key recovery procedures and instructions for using the BCP and the emergency response guidelines;
- Potential IT infrastructure loss scenarios.

► BCPs are updated when necessary, and communicated to all concerned associates.

PC-80-30-010-030

[Risk(s): Crisis management; Performance gap]

► The appropriateness, effectiveness and efficiency of BCPs is checked regularly in tests and exercises (especially the possible loss of IT infrastructure). Results of these tests and exercises are kept to allow historical analysis.

PC-80-30-010-040

[Risk(s): Crisis management; IT asset damage; Performance gap]

► To ensure Business Continuity, IT department has:
- sufficient resources (e.g. IT staff and equipment) to ensure that the running of network platform/applications/shared drives are without any delays and disruption;
- evaluated accessibility to physical IT assets by IT staff;
- defined a priority setting system for IT requests;
- ensured that equipment assigned to staff are properly registered on IT register (and duly returned if need be);
- forbidden the use of personal devices (laptop, smartphone, tablet, etc.) to access Sonepar's systems and network.

PROCESS:

MANAGE SECURITY AND SAFETY OF PEOPLE AND ASSETS

ACTIVITIES

Manage HSE and insurable risks

PC-80-40-030-010

[Risk(s): Health and safety]

► An HSE (Health, Safety & Environment) strategy is set up and validated annually by the local top management outlining
- specific objectives and goals based on HSE policies;
- HSE organization;
- HSE accountabilities and responsibilities;
- HSE risk management;

- HSE training plan;
- HSE performance review;
- HSE documentation.

PC-80-40-030-020

[Risk(s): Health and safety]

► A yearly Safety plan is prepared and updated in each business location by the appropriate level of management and validated by local top management. Its aim is to define the main actions regarding safety, based on a risk analysis (identification of main local risks concerning health & safety of associates) and local health & safety laws.

► Therefore, safety plan:

- includes a risk Assessment / business impact analysis;
- takes into account locally applicable health, safety and environment regulations;
- specifies required inspections and controls of equipment, tools and assets;
- details the whole process to manage risks induced by contractors' activities;
- specifies duties and tasks assigned to each individuals involved in the process (prevention, detection and emergency measures).
- Each OPCO ensures that the safety plan is communicated to all their associates.

PC-80-40-030-025

[Risk(s): Health and safety; Performance gap]

► Each OPCO ensures that 5S practice (workspace organization method) is implemented and maintained to all sites, including a training plan to all associates.

PC-80-40-030-030

[Risk(s): Health and safety]

► Local top management ensures associates' training and awareness by organizing training and regular communication on work place, covering at least the following topics:

- Equipment, tools and assets are regularly inspected and maintained as per local regulations and Group standards (firefighting equipment, housekeeping, pallets and racks, forklifts, trucks...);
- Cable machines are designed, positioned, checked and maintained according to local regulations and risk assessment. They are equipped with an emergency stop and with safety guards or protective devices intended to prevent the operator from coming into contact with moving parts;
- Smoking is forbidden in all Sonepar stock areas and each company must comply with local laws related to smoking in the workplace and in public places;
- All associates are provided with Personal Protective Equipment (PPE) pertaining to the occupational risks to which they may be exposed to. Managers enforce the PPE rules for all concerned associates (counter & warehouse associates…) and third parties working in these areas;
- Physical access to headquarters, main storage areas and IT centers is adequately monitored.

PC-80-40-030-040

[Risk(s): Health and safety]

► Safety is tested (with exercises) at least once a year by third parties / professionals unaffiliated with the Company.

► Results of annual safety test are formally documented by local management. Any additional risks or process deficiencies are identified and addressed with changes to safety plan.

► Safety plan is updated subsequently and reviewed by local top management.

PC-80-40-030-050

[Risk(s): Health and safety]

► Deviations from good practices and Sonepar rules in terms of health and safety are identified and a remediation plan is set up and followed by local top management.

PC-80-40-030-060

[Risk(s): Health and safety; Misappropriation of assets]

► In accordance with Group standards, HSE (Health, Safety & Environment) KPIs are reported to the Group Risk and Insurance department on a quarterly basis.

NEW PC-80-40-030-070

[Risk(s): Health and safety]

► The 12 Golden Safety Rules are applied locally (see appendices).

► Awareness and training workshops are organized at local level.

PC-80-40-030-080

[Risk(s): Business non-compliance]

► CFO or local Risk Manager ensures that the entity's assets are correctly covered by Group insurance by checking that:
- insurance report is sent to the entity by the SVP Risk and Insurance;
- report is reviewed periodically to ensure that Group insurance covers all assets of the entity;
- deficiencies (between the entity's assets and assets insured by the Group) are reported to the SVP Risk and Insurance.

PC-80-40-030-085

[Risk(s): Business non-compliance]

► The Group Insurance strategy is properly communicated and applied, at local level.

PC-80-40-030-090

[Risk(s): Business non-compliance]

► Insurance policies must be implemented to cover physical damages, general and professional liability, cyber risks, Directors & Officers liability, employment practices liabilities, cargo and transportation, special risks, business travel, fraud/crime and credit risk. These policies must be the Group global ones managed by the Group global insurance broker. Use of local policies for these insurance lines (exception given according to context) must be approved by the General Counsel. Other non-life insurance lines (motor, etc.) can be taken out locally.

PC-80-40-030-100

[Risk(s): Business non-compliance]

► In case of event or a claim that may trigger insurance policies, notifications must be appropriately and timely made in compliance with Group's agreed terms.

PC-80-40-030-110

[Risk(s): Health and safety; Logistic infrastructure]

► Locations inventory and evaluation (i.e. building, stocks, other properties..) are performed once a year as part of the annual updating campaign managed by the SVP Risk and Insurance.

PC-80-40-030-130

[Risk(s): Performance gap]

► There is a follow up on the total cost of risk: deductibles in case of loss or claim, reinvoicing on cost of insurance (through management fees), losses and claims management costs…

PC-80-40-030-140

[Risk(s): Health and safety; Logistic infrastructure]

► Any new installation of photovoltaic panels on-premises is subject to:
- a declaration to the Group risk and Insurance department;
- a project review organized with an external risk engineering company appointed by the Group;
- prior approval from Group insurance team and insurers.

PC-80-40-030-150

[Risk(s): Health and safety; Logistic infrastructure]

► Recommendations issued by the external risk engineering company during audits of CDCs are implemented timely and reported to Group insurance team (if applicable).

PC-80-40-030-160

[Risk(s): Health and safety; Logistic infrastructure]

► "Hot work permit" (needed to use flames or produce heat/sparks, even temporary, as welding or grinding) procedures are systematically implemented in entity premises, in accordance with local legislation and Group guidelines. They are revised when necessary.

PC-80-40-030-170

[Risk(s): Health and safety; Logistic infrastructure]

► Fire Protection System Impairment procedures are systematically implemented in premises equipped with sprinkler systems, in accordance with local legislation and Group guidelines. In case of rental of the premises, it must be ensured with the owners that local legislation and Group guidelines are properly respected. These procedures are regularly reviewed and revised as needed.

PC-80-40-030-180

[Risk(s): Health and safety; Logistic infrastructure]

- ► Any Warehouse, Central Distribution Center, or Regional Distribution Center greenfield or brownfield construction or renovation project is subject to:
  - a preliminary declaration to the Group's Risk and Insurance department;
  - a project review organized with an external risk engineering company appointed by the Group.
- ► This also applies to any new installation of an Automated Storage and Retrieval system (Autostore, Knapp, Mecalux, Witron…) in existing premises.

ACTIVITIES

Respect Human Rights

PC-80-40-040-010

[Risk(s): Human rights own workforce; Value chain workers rights; Corporate culture]

- ► The Human Rights policy - along with other Group tools (e.g. Unified Risk Mapping) - is made available locally, spread and translated if needed in order to ensure proper awareness.

PC-80-40-040-020

[Risk(s): Human rights own workforce; Value chain workers rights]

- ► Risks identified during the Unified Risk Mapping process (if any) are properly and timely mitigated.

PROCESS:

ENHANCE GENERAL CONTROL ENVIRONMENT

ACTIVITIES

Maintain clear organizational structure

PC-80-50-010-020

[Risk(s): Executive management; Authority/limit]

- ► The entity establishes appropriate lines of reporting, given its size and the nature of its activities.
- ► An organization chart, defining each position, is implemented in each business location and in each Department, and validated by local top management.
- ► Organization charts are communicated to all associates.
- ► Organization charts are updated when necessary and reviewed by local top management at least annually.

PC-80-50-010-050

[Risk(s): Skills and knowledge capital; Executive management]

- ► Each job role in the company is associated with a job description and appropriate accountabilities definition.

PC-80-50-010-060

[Risk(s): Performance gap; Executive management]

- ► There is a regular review and monitoring of all corporate legal entities of the perimeter and efforts are made to maintain them at a reasonable number.

PC-80-50-010-070

[Risk(s): Authority/limit]

- ► All legal entities' name or scope changes need prior approval of Sonepar General Counsel and the Chief Communication Officer.

ACTIVITIES

Monitor internal control

PC-80-50-050-005

[Risk(s): Business non-compliance; Performance gap]

- Sonepar Internal Control Manual is communicated to every OPCO of the Group and made available to every associate.

PC-80-50-050-006

[Risk(s): Business non-compliance; Performance gap]

- There is an annual Representation letter signed by the CEO and CFO of the country sent to the Group CEO and Group CFO (see appendices).
- On the financial statement part, it is supported by the Forms templates for representation letters that are completed three times a year.

PC-80-50-050-007

[Risk(s): Business non-compliance; Performance gap]

- There is an Internal Control annual report by the CFO of the country sent to the Group CFO (see appendices).

PC-80-50-050-010

[Risk(s): Business non-compliance; Performance gap]

- A documented internal control self-assessment process is implemented by Corporate Management.
- Internal control deficiencies are reported by local management through self-assessment process, or each time it is deemed necessary.
- Remediation plans are implemented and followed by local top management.

ACTIVITIES

Manage compliance with internal audit standards

PC-80-50-060-010

[Risk(s): Business non-compliance; Authority/limit]

- Management gives to internal auditors full and free access to Sonepar records and data, personnel and locations relevant to the performance of their audit engagements.
- The necessary documentation and data are communicated to internal auditors prior to audit fieldwork as mentioned in the engagement letter.
- The top management of the audited entity is available for the closing meeting organized at the end of every audit engagement fieldwork.
- During this meeting, the audit team provides top management with its findings and recommendations which are formally discussed.

PC-80-50-060-040

[Risk(s): Business non-compliance; Performance gap]

- From internal audit's finding and recommendations, the top management of the audited entity must develop their actions in a timely manner with an owner and a deadline.
- The top management of the audited entity is then responsible for reporting to Internal Audit on the follow-up of the implementations of its actions.

ACTIVITIES

Manage compliance with external audit standards

PC-80-50-070-010

[Risk(s): Business non-compliance; Accounting information]

- Local top management ensures that external auditors issue a full scope audit opinion at country level. Local and OPCO management will comply with Group audit instructions and reporting deadlines.
- Local top management responds timely and appropriately to the findings and recommendations of the external auditors.
- Any significant audit issue arising before or during the year-end audit is immediately reported to executive management and to the country's board of directors along with Sonepar SVP Audit.

PC-80-50-070-050

[Risk(s): Business non-compliance; Accounting information]

- Local top management ensures that external auditors communicate their findings and recommendations regarding internal control, policies and procedures in writing. Action plans for remediation are developed and addressed in a timely fashion.

ACTIVITIES

Ensure compliance with company code of conduct

PC-80-50-080-010

[Risk(s): Business non-compliance; Corruption]

- Each OPCO top manager has taken all the necessary steps as the case may be, with the help of his/her Legal, Compliance and HR Departments, to include the Group Code of Conduct and the Compliance Manual in his/her OPCO policies or other internal rules (included, if needed, a prior consultation of workers' council or a local board approval).
- Local Codes of Conduct and local policies and procedures have been updated and/or implemented to reflect the standards and rules set by the new Group Code of Conduct and the Compliance Manual.
- Appropriate information and education are offered to associates for a proper understanding of the Code of Conduct and the Compliance Manual.
- Acknowledgement to the Group Code of Conduct has been signed by each associate.

PC-80-50-080-020

[Risk(s): Business non-compliance; Corruption]

- Each OPCO top manager removes or reduces incentives or temptations that might cause personnel to engage in dishonest or unethical acts.

PC-80-50-080-030

[Risk(s): Business non-compliance; Corruption]

- Each OPCO top manager monitors non compliance with the Code of Conduct, the Compliance Manual and other group policies and takes appropriate disciplinary actions.

ACTIVITIES

Pilot board management

PC-80-50-090-040

[Risk(s): Executive management; Authority/limit]

- Board meetings and shareholders' meetings are organized and held in compliance with local law and Sonepar Governance Charter.
- Directors are appointed in compliance with the Approval Matrix.
- Solis company database is updated regularly.

PC-80-50-090-120

[Risk(s): Business non-compliance; Executive management]

- Agendas of Group Board meetings are systematically drafted and circulated. They systematically cover compliance.
- Minutes of meetings (board and shareholders) are systematically and promptly drafted in compliance with local law, reviewed by legal department (or identified personnel), approved and filed in Solis company database.

ACTIVITIES

Implement / maintain a whistleblowing process

PC-80-50-110-010

[Risk(s): Business non-compliance; Corruption; Third-party non-compliance]

- Each OPCO ensures that the Speak Up Policy as available in the Compliance Manual has been communicated to all associates and is available on the local intranet.
- Reports made outside of Sonepar Reporting Platform (e.g., directly to the manager, to HR, through emails or mails) are included in Sonepar Reporting Platform by the legal team.
- Complaints or concerns raised to the OPCO or Country top management included corruption and influence peddling are investigated. If necessary, corrective actions are implemented and disciplinary actions taken.

ACTIVITIES

Prevent and manage corruption

PC-80-50-120-010

[Risk(s): Business non-compliance; Corruption]

- The Corruption and Influence Peddling Risk Mapping is updated, regularly as per Group's methodology, with local inputs and assessments (impact/ frequency/level of control) and remediating actions are implemented if needed.

PC-80-50-120-020

[Risk(s): Business non-compliance; Corruption]

- Trainings on corruption and influence peddling are organized regularly for all exposed associates.

PC-80-50-120-030

[Risk(s): Third-party non-compliance; Corruption]

- Charters dealing with corruption risk are implemented for sales and purchasing teams within the company.

PC-80-50-120-060

[Risk(s): Business non-compliance; Corruption]

- Sponsorships and Charitable Donations are made in compliance with the Compliance Manual and the dedicated Regional Policy.
- They are monitored annually by the Finance/ Business controlling department.
- Independent control is in place and maintained locally to ensure the absence of conflict of interests in particular from the top management.

PC-80-50-120-100

[Risk(s): Business non-compliance; Corruption; Third-party non-compliance]

- Code of Conduct and the Compliance Manual are communicated and implemented locally. The Regional Policy has been drafted, implemented and communicated as per the rules set in the Compliance Manual.

PC-80-50-120-110

[Risk(s): Third-party non-compliance; Corruption; Value chain workers rights]

- In accordance with the Compliance Manual, a formal Business Partner Assessment procedure is established at Country level, approved and supervised at Regional and Group level and implemented in the OPCOs and Shared Service Centers.
- This procedure includes the definition of assessment criteria (incl. respect of Human Rights, corruption risk exposure etc.), the setup of a risk scoring matrix and the specification of due diligence by category and risk level.
- The Group "Procedure applicable to Intermediaries", established for submitting, assessing and approving Intermediaries, is strictly followed. It is translated into a local operating procedure, which also includes the monitoring process of operations with intermediaries.

PC-80-50-120-115

[Risk(s): Third-party non-compliance; Corruption]

- All Business Partners' alerts (e.g. bad press, change in leadership etc) are reviewed and acted upon on a regular basis and no back log alert can exceed 3 months.
- Status of Business Partner Assessment is up to date according to such changes (which could have an impact on Business relationship).

PC-80-50-120-120

[Risk(s): Third-party non-compliance; Corruption]

- Each Country monitors the number of active Business Partners by category, noting which partners were subject to a due diligence, approved, deferred and rejected.
- These KPIs are reported to the SVP Risk and Insurance bi-annually.

PROCESS:

MANAGE ENVIRONMENTAL SOCIAL AND GOVERNANCE REQUIREMENTS

ACTIVITIES

Manage environmental social and governance requirements

PC-80-60-010-001

[Risk(s): Sustainability strategy execution]

- A dedicated CSR organization and governance is in place, covering the full scope of activities. It identifies and includes key functions (such as Human Resources, Legal and Compliance, Risks, Sustainability, Health & Safety) to organize and ensure effective CSR awareness, actions, compliance and reporting.
- Contributors understand their roles and are allocated the necessary time to complete their tasks. They receive training on CSR principles and the necessary tools (such as kShuttle for reporting purposes).

PC-80-60-010-002

[Risk(s): Extra-financial reporting]

- Data quality checks are implemented to ensure transparency and adequacy of the reported quantitative and qualitative data, in respect of the definitions and rules formalized and updated in the CSR reporting tool. These checks are performed before validation in the CSR reporting tool.

PC-80-60-010-003

[Risk(s): Extra-financial reporting]

- CSR Group Action Plans, resulting from the IROs (Impact, Risks and Opportunities) of the double materiality analysis, are duly implemented at the local level. If necessary, these plans can be reinforced with additional locally initiated actions.

PC-80-60-010-010

[Risk(s): Extra-financial reporting]

- In coordination with the SVP Sustainability, each country and OPCO will monitor and analyze, the measurements of their: CO_2 emissions, water consumption and waste level. The presentation of the CO_2 reduction solutions (with KPIs monitoring) is part of the country/OPCO board presentation.

PC-80-60-010-015

[Risk(s): Extra-financial reporting]

- Planet and People Key Performance Indicators (KPIs) and associated actions defined in Sonepar's Purpose bold commitments are evaluated at the country level and reported to the Group on an annual basis. These KPIs are monitored locally on a regular basis.

PC-80-60-010-020

[Risk(s): Corporate culture; Circularity]

- As part of the Energy Transition Academy, all concerned associates have followed the Sustainability (aligned with Sonepar's Purpose) and Circularity e-learnings.

PC-80-60-010-030

[Risk(s): Circularity; Pollution]

- There is a formalized process, defined at OPCO level, for collecting (and recycling) customers' electrical and electronic equipment wastes. If applicable, measurements are followed and monitored.

PROCESS:

ENSURE APPROPRIATE COMMUNICATION

ACTIVITIES

Manage crisis (in case of reputational risk for the Group)

PC-80-70-010-010

[Risk(s): Communication; Crisis management]

► Sonepar President and CEO, Regional President General Counsel and Sonepar Chief Communications Officer are immediately informed in case of potential crisis. A local crisis communication process is in place and circulated at appropriate level.

ACTIVITIES

Manage corporate communications to journalists, radio & TV

PC-80-70-020-030

[Risk(s): Communication]

► Any public positions on any politically sensitive topics receive prior approval from Chief Communications Officer & General Counsel.

ACTIVITIES

Establish communications plan

PC-80-70-030-010

[Risk(s): Communication]

► There is a written document that clearly states the communications plan for the country / OPCO. It follows the directives of the Group communications plan as presented in the International Communications Committee.

ACTIVITIES

Manage local communication with significant Group impact

PC-80-70-040-010

[Risk(s): Communication]

► Any local business communication with a significant Group impact (reputation, image) needs to be approved beforehand by the OPCO or Country top manager before being sent to the Chief Communications Officer & General Counsel for second approval.

ACTIVITIES

Publicly communicate financial information

PC-80-70-050-010

[Risk(s): Communication]

► Only figures that are already published externally by the Group can also be communicated at Region, Country or OPCO levels, after approval by Sonepar CFO.

ACTIVITIES

Create web sites / social media accounts / intranets

PC-80-70-060-010

[Risk(s): Communication; Intellectual property]

► Any new website, new social media account or new intranet developments for a Country or OPCO needs approval of Chief Communications Officer before going live.

► All Intranets must use Microsoft SharePoint modern.

PC-80-70-060-020

[Risk(s): Communication]

► Group Social Media Guidelines are made available to all associates, at least digitally. Local guidelines may exist and be used if covering at least Group aspects.

PC-80-70-060-030

[Risk(s): Intellectual property; Cybersecurity]

► Locally, a policy regarding registration and management of domain names is formalized, including:
- the preventive/defensive choice to buy (or not) similar extensions/domain names;
- the surveillance principles, including the renewal watch (in order not to lose the extensions) and the review of similar domain names used by third parties;
- the registration principles: a domain name shall only be registered by the OPCO using the domain name or if the domain name includes a Global trademarks (i.e., "SONEPAR" or "POWERED BY DIFFERENCE"), the owner shall be SONEPAR SAS. Domain names cannot be registered by third-parties, suppliers, partners, external consultants;
- prior approval of HQ's Communication Department is requested in case of registration of a domain name which include Global trademarks.

► A full list of all local domain names used/bought exists, is reviewed and updated on a regular basis. This list is shared with the Group General Counsel each year.

ACTIVITIES

Manage marketing communication

PC-80-70-070-010

[Risk(s): Communication]

► Any branding or marketing communication campaign that may significantly affect the Group's image or brand value needs to be approved beforehand by the OPCO or Country top manager before being sent to the Chief Communications Officer for second approval.

PC-80-70-070-020

[Risk(s): Communication]

► All logos of OPCOs as endorsed brands include "A Sonepar Company" baseline. All logo creations or updates need prior approval of the Chief Communication Officer and must follow the Group Logo Creation Governance.

PC-80-70-070-030

[Risk(s): Communication; Intellectual property]

► The creation and/or registration of new brands and logos, the use of Sonepar trademarks by any third party (except use of logo for usual reference lists) and any legal action to protect Sonepar trademarks (infringement) is approved beforehand by the Group General Counsel and the Chief Communications Officer.

► The use of Sonepar as a commercial brand is approved beforehand by the Chief Communications Officer.

PC-80-70-070-040

[Risk(s): Communication]

► The global and local use of the Sonepar brand complies with the Sonepar Brand Standards available in the Brand Hub: brand.sonepar.com

ACTIVITIES

Manage right to publish

PC-80-70-080-010

[Risk(s): Communication]

► Countries and OPCOs have in place clear defined roles and responsibility of who has the right to publish information on internal (intranets, yammer) and external channels (internet, social media).

Revision History

REVISION DATE	NATURE OF CHANGES
2016-05	▶ Include revised ICT policy (V3.1) ▶ Update Standards and Best practices
2018-03	▶ Include revised ICT policy (V4) ▶ Update Standards and Best practices
2019-02	▶ Add Appendices • Business Partner Assessment • Internal Control declaration (new template) • Fraud, Corruption & Influence Peddling report (new template)
2020-04	▶ Alignment with new Group Code of Conduct and the latest Corruption and Influence Peddling Risk Mapping ▶ New format ▶ Update of existing Control Points ▶ Add new Control Points on core topics
2021-03	▶ New format ▶ Definition of key controls ▶ Rewording of some Control Points and addition of new ones
2022-03	▶ Mapping of the Control Points with the Group Risk Mapping ▶ Rewording/merger/update of some Control Points and addition of new ones (mostly on IT security and GRC)
2023-04	▶ Change in the Supply Chain Macro Process ▶ Rewording of some Control Points and addition of new ones
2024-03	▶ Alignement with IT security Golden Rules ▶ New tags on Sapin 2, Cybersecurity and new Control Points ▶ Rewording of some Control Points and addition of new ones
2025-03	▶ New tag on CSR Control Points and new dedicated process ▶ Risks identified below each Control Point ▶ Rewording of some Control Points and addition of new ones (mainly Supply Chain planning)
2026-02	▶ Rewording of some Control Points and addition of new ones ▶ Reorganization of the Sales & Marketing, Purchasing and Finance Macro-Processes

sonepar
Powered *by* **Difference**

SONEPAR SAS
25, rue d'Astorg
75008 Paris - France
Tel. :+33 (0)1 58 44 13 13

sonepar.com