4

Risk factors and management

AFR

Investors are advised to consider all of the information provided in this Universal Registration Document, including the risk factors described in this section, before making their investment decision. The described risks are those, as of the date of this document, which the Company believes are specific to it and whose occurrence could have a material adverse impact on the Group, its business, financial position, results of operations or development.

The main risks together with the measures for managing these risks are described in section 4.1 below.

Legal and arbitration proceedings are described in section 4.2, page 78.

Measures for transferring risk are described in section 4.3, page 79.

Internal control and risk management procedures are described in section 4.4, page 80.

4.1 Risks and measures to manage the risks

The risks and threats to the Group's business are reviewed regularly, under the supervision of the Audit and Risks Committee. Group risk mapping involves identifying and assessing nearly 200 risks based on a number of criteria, including likelihood of occurrence, financial impact and reputational impact for the purpose of evaluating the "gross" risk (*i.e.*, "net" of existing risk management procedures). The effectiveness of risk management procedures then has to be analyzed to evaluate the "net" risk materiality.

In 2020, these risks were tracked by the Audit and Risks Committee so that the related action plans could be updated in line with any change. Thanks to the increasingly digital nature of its solutions, the Group's operations proved relatively resilient.

However, action plans and risk monitoring were adapted to factor in the economic slowdowns observed in the wake of the measures taken to contain the Covid-19 epidemic in the 46 countries where the Group operates. The Group reacted to the consequences of the epidemic notably by adjusting its monitoring of business continuity, customer counterparty and voucher fraud risks.

These adjustments in light of the Covid-19 epidemic were incorporated into the five categories of risk included in the mapping process shown below. They are classified in descending order of importance within each category. This updated analysis does not reveal any specific new risks, nor any material change in risk levels compared to 2019.

SUMMARY TABLE OF RISK FACTORS

Net impact:	● : Low	● ● : Medium	● ● ● : High
Net probability:	● : Low	● ● : Medium	● ● ● : High

Category	Risk factors and related sections		Probability	Impact	Related extra-financial priority issues
Financial Risks	Currency risk	4.1.1.1	● ● ●	● ● ●	
	Tax risk	4.1.1.2	● ●	● ● ●	
	Commodity risk	4.1.1.3	● ●	● ●	
	Customer counterparty risk	4.1.1.4	● ●	● ●	
	Financial institutions counterparty risk	4.1.1.5	●	● ●	
Legal risks	Risks related to changes in the laws or regulations governing solutions qualifying for a specific payroll and/or income tax regime	4.1.2.1	● ●	● ● ●	
	Risks related to competition law	4.1.2.2	● ●	● ● ●	**Business ethics** (5.4.1.1) **Personal data** (5.4.2.2)
	Risks related to personal data protection regulations	4.1.2.3	● ●	● ● ●	
	Risk related to enhanced regulatory oversight over the Group's activities via banking regulations	4.1.2.4	●	● ●	
	Risks related to corruption, money laundering and / or terrorist financing schemes	4.1.2.5	●	● ●	**Business ethics** (5.4.1.1)
Information systems and cybercrime risks	Information system risks	4.1.3.1	● ●	● ● ●	**ITsecurity** (5.4.2.1) and **Personal data** (5.4.2.2)
	Cybercrime risks	4.1.3.2	● ●	● ● ●	
Group strategy and competitive environment risks	Competitive environment risks	4.1.4.1	● ●	● ● ●	
	Risks related to the acquisition strategy	4.1.4.2	●	● ●	
	Risks related to the partnership strategy and other strategic agreements	4.1.4.3	●	● ●	
Operational risks	Business continuity risks	4.1.5.1	● ●	● ●	
	Voucher fraud risks	4.1.5.2	● ●	● ●	

Non-financial risks, which were not among the main risks identified in the review, are qualified as secondary risks. They are presented in section 5.1.4 "Non-financial risk analysis" based on the Group's risk mapping methodology. These secondary non-financial risks were assessed as non-material in terms of their short-term financial impact and the control over these risks by the departments concerned. They include climate change and risks related to talent attraction and retention. It should be noted that, although Covid-19 did not emerge as a specific and material risk in the 2020 review of the Group's main risks, the epidemic and an assessment of its impacts are discussed in section 2.1.8 "Main risks and uncertainties".

4.1.1 Financial risks

The main financial risks to which the Group is exposed are as follows:

- currency risk, described in section 4.1.1.1, see below;
- tax risk, described in section 4.1.1.2, see below;
- commodity risk, described in section 4.1.1.3, see below;
- customer counterparty risk, described in section 4.1.1.4, see below;
- financial institutions counterparty risk, described in section 4.1.1.5, see below.

Detailed quantified information about the Group's exposure to these risks, after hedging, is presented in Note 6.6 to the consolidated financial statements, page 260.

The Group's financial risk management policy is designed to meet the following core objectives (listed in order of priority): financial security of transactions, liquidity of assets and sources of financing, and profitability (interest income and expense). The aim is to minimize the impact of market risks on the Group's results and, to a lesser extent, on the balance sheet. Interest rate and currency risks are managed at the Group level by the Treasury & Financing Department, which reports to the Executive Vice-President, Finance.

Interest rate and currency instruments are used to support the Group's investment and financing policies, as well as its hedging strategies (fair value and cash flow hedges). Group Treasury and Financing has the necessary expertise and computer applications (Front to Back treasury management software) to invest available cash, raise funds and hedge risks on the financial markets in accordance with the practices generally applied by leading groups. The department's organization and procedures are reviewed by the Internal Audit Department. Monthly cash reports are submitted to the Executive Vice-President, Finance, who validates the objectives set in accordance with previously approved management strategies.

Despite the Covid-19 epidemic, liquidity risk remains non-material. It is discussed in Note 6.6, "Liquidity risk", to the consolidated financial statements, page 263.

4.1.1.1 Currency risk

Risk

The Group is exposed to currency risks on the translation into euros in the consolidated financial statements of business volumes, revenue, EBIT and balance sheet items for each country outside the euro zone. Due to the Group's operations in 46 different countries, many financial statement indicators are inevitably exposed to foreign currency translation risk, particularly that arising from the translation of financial statements denominated in Brazilian reals and Mexican pesos. A significant proportion of the Group's business is generated in countries where the functional currency is different from the Group's reporting currency (the euro).

However, the Group is only exposed to limited currency risk, because each subsidiary's revenues and expenses are generated and paid in local currency.

Actual cash flows between countries whose currency is not the euro consist mainly of dividends and royalties paid by subsidiaries to their parent company, and interest payments made and received on intercompany financing. These cash flows may be exposed to changes in exchange rates between the original currency and the euro.

Exchange gains and losses recognized in the 2020 income statement are presented in Note 6.1 "Net financial expense" to the consolidated financial statements, page 251.

The impact of a 10% change in the exchange rates of the main currencies is presented in Note 6.6 to the consolidated financial statements, paragraphs "Foreign exchange risk: currency analysis", "Currency hedges" and "Sensitivity to exchange rates", page 262.

Measures to manage the risk

Group policy consists of investing the cash generated by an activity in the currency of the country that manages said activity. This avoids having to manage the liquidity risk associated with currency fluctuations and reduces currency risk exposure.

This foreign currency translation risk is not hedged.

However, concerning currency risks on capital flows between subsidiaries and the parent company, foreign currency loans/borrowings are translated using the standards generally applied by leading groups. Other capital flows are included in the monthly cash reports presented in the preliminary comment in section 4.1.1.

4

Neither Edenred S.A. nor the Group has any open currency positions that would be likely to expose the Group to significant risks.

At December 31, 2020, the Company did not have any cash flow hedges of currency risks concerning forecast capital flows maturing in less than 12 months for limited notional amounts.

4.1.1.2 Tax risk

Risk

As an international group, Edenred is subject to the tax laws of a large number of countries and conducts its business in compliance with various regulatory requirements. The tax rules in force in the Group's various host countries do not always provide clear solutions that are unequivocal in meaning. As a result, the Group's organisational structure, the way it conducts business and the applicable tax regime are based on its own interpretation of local tax rules. There is no guarantee that its interpretations will not be challenged by local tax administrations in the future.

The Group is currently involved in various tax disputes. These are described in Note 10.3 "Claims, litigation and tax risk" to the consolidated financial statements, page 282.

Measures to manage the risk

Assisted by the legal and tax departments and/or a firm of legal and tax advisers, the subsidiaries ensure that they comply with local tax rules.

4.1.1.3 Commodity risk – fuel

Risk

Part of Edenred's business model is sensitive to fluctuations in fuel prices in the different countries in which it provides Fleet & Mobility Solutions. Indeed, some of these solutions are fuel cards used to pay for fuel. The commission received by Edenred for these products is sometimes partly dependent on fuel prices. Fuel prices are determined based on a number of factors, including the price of crude oil and the level of local taxes. Dependence on crude prices varies significantly both by country and by solution. In 2020, 9% of the Group's total revenue was sensitive to oil price fluctuations. The sensitivity of the Group's total revenue to a 10% change in oil prices – based on Brent Crude for Europe, and Brent Crude and West Texas Intermediate (WTI) Crude for Latin America – is estimated at €7 million.

Measures to manage the risk

In Fleet & Mobility Solutions, Edenred has developed a large portfolio of non-fuel-based value-added services, driven either by organic growth or acquisitions. For example, UTA, in which Edenred holds an 100% stake, has a highly diversified revenue model based on toll, parking, vehicle maintenance payment and other solutions. This drive to develop fleet and mobility solutions that go beyond fuel accounts for the leadership position Edenred now holds in the vehicle maintenance sector in Brazil. The Group has also refined its pricing strategy – country by country, and solution by solution – to reduce revenue exposure to fuel price fluctuations.

In addition, Edenred contracts commodity hedges to hedge against unfavourable changes in fuel prices in Europe. Those instruments represented a cumulative notional equivalent amount of €5 million at the period end. New instruments have been added to the portfolio to partially hedge revenues for 2021. These hedging instruments are described in Note 6.6 "Financial instruments and market risk management", to the consolidated financial statements, page 265.

4.1.1.4 Customer counterparty risk (credit risk)

Risk

Customer counterparty risk – or credit risk – essentially concerns the risk of customers being unable to honour amounts that they owe to the Group. This could apply to post-payment facilities where invoicing is based on the volume consumed and not the issue volume. This is the case for Fleet & Mobility Solutions, for example, as well as for payment terms extended to prepaid solution customers where invoicing is based on the issue volume.

The significant proportion of business generated by – generally prepaid – Employee Benefits and Complementary Solutions (Incentive & Rewards) limits the Group's exposure to credit risk. However, Fleet & Mobility Solutions, where about 25% of 2020 business volume was pre-loaded, tends to increase the Group's credit risk exposure.

Edenred's exposure to a major customer default is a contained risk. Because the statistical dispersion of the business throughout the 46 countries where the Group operates is high, no customer billed in 2020 represented a significant share of revenue. In addition, trade receivables correspond to several hundreds of thousands of accounts.

Measures to manage the risk

Thanks to an assertive collection policy, the Group has reduced trade receivables days. Although economic indicators show that business default rates have improved due to government support in most of the regions where the Group operates, the Group has factored in an increased credit risk when calculating provisions for trade receivables in certain regions with higher macroeconomic risk.

Most subsidiaries have set up dedicated teams to manage this risk, and use external databases to assess the financial health of prospects or customers.

Some country organizations have chosen to implement risk transfer solutions, notably in the form of credit insurance, especially for post-payment facilities and in markets where there is a demand for longer payment periods.

Moreover, as part of the Next Frontier strategic plan, the Group is accelerating the development of its SME client base, thereby helping to diversify customer risk even further.

4.1.1.5 Financial institutions counterparty risk

Risk

The Group is exposed to banking counterparty risk, especially with regard to funds invested. Its counterparties are financial institutions with which its available cash is invested and from which interest rate and currency instruments are purchased. Default by one of these institutions or a deterioration in its financial position could result in financial losses for Edenred.

Measures to manage the risk

Exposure to counterparty risk is reduced by dealing only with leading counterparties according to correlated country risks. The Group uses a wide range of counterparties, sets exposure limits by counterparty and uses a monthly reporting procedure to track their concentration and their credit quality based on their credit ratings.

Details of the Group's counterparties are presented in Note 6.6 "Financial instruments and market risk management" to the consolidated financial statements, paragraph "Credit and counterparty risk", page 265.

Group policy consists of investing available cash in the currency of the country in which its solutions are proposed. It is therefore exposed to country risks, which could, in particular, arise from a financial crisis affecting one or more of its host countries.

A significant proportion of the Group's available cash (corresponding to cash denominated in euros) is invested with the holding company, Edenred S.A., under the worldwide centralized cash management scheme. Under this system, the subsidiaries' available cash is transferred to Edenred S.A. in all cases where this is allowed under local law or the law governing the business concerned, and where financial conditions permit. Regular centralized monitoring of these funds helps to reduce the Group's exposure to counterparty risks on the leading financial institutions with which the funds are invested.

Moreover, pooling available cash in this way is one of the main reasons for the Group's very limited exposure to counterparty risks in countries on review for a potential credit rating downgrade. As part of this prudent policy, the Group selects financial institutions independently of the country from which the available cash originates.

Invested funds amounted to €4,724 million at December 31, 2020, of which €2,146 million (gross) reported as cash and cash equivalents and other marketable securities (see Note 6.3 "Cash and cash equivalents and other marketable securities" to the consolidated financial statements, page 253) and €2,578 million reported as restricted cash (see Note 4.7 "Change in Restricted cash", page 241).

The average interest rate was 1.3% at December 31, 2020 and 1.9% at December 31, 2019. Instruments with maturities (after any hedging) of more than one year represented 22% of the total at December 31, 2020 *versus* 27% at December 31, 2019.

4.1.2 Legal risks

The five main legal risks to which the Group is exposed are as follows:

- risks related to changes in the laws or regulations governing solutions qualifying for a specific payroll and/or income tax regime, presented in section 4.1.2.1 below;
- risks related to competition law, presented in section 4.1.2.2 below;
- risks related to personal data protection regulations, presented in section 4.1.2.3 below;
- risk of tighter control over the Group's activities *via* banking regulations, presented in section 4.1.2.4 below;
- risk of being caught up in activities that involve bribery, money laundering and/or the financing of terrorism, presented in section 4.1.2.5 below.

4.1.2.1 Risks related to changes in the laws or regulations governing solutions qualifying for a specific payroll and/or income tax regime

Risk

Some Group solutions are governed by national regulations designed to create a dedicated legal framework (mainly for payroll tax, income tax) that will encourage their development. They are mainly Employee Benefits, particularly *Ticket Restaurant* and *Ticket Alimentación*. In 2020, Employee Benefits accounted for 61% of the Group's operating revenue.

These laws and/or regulations may change in ways that are unfavourable to the Group. For example, governments in certain countries may be tempted to scale back or abolish the payroll tax or income tax benefits attached to these solutions. As the solutions' income and payroll tax appeal and the rules restricting their use to specific purposes are core factors behind their growth, any unfavourable change in the regulatory or legislative environment could lead to a decline in related business volume.

See section 1.5 "Regulatory environment", page 31, for more information about the regulations applicable to the Group, including sections 1.5.2.1 and 1.5.2.2, pages 32 et 33, which describe the regulatory environments in France and in Brazil, respectively.

Measures to manage the risk

The Public Affairs Department implements targeted measures on behalf of the Group, such as:

- continuously monitoring political, social and economic developments in the Group's host countries in order to be forewarned of proposed changes in the laws and regulations applicable to solutions that qualify for a specific payroll tax or income tax regime;
- developing institutional tools, such as macro-economic studies, research, surveys and position papers, demonstrating the effectiveness of Edenred's solutions in promoting specific policies;
- identifying the core players in government, government departments, the corporate world and academia that are involved at the international, the European and the national level, and developing long-term contacts with them;
- participating in public debate, in order to remain a preferred contact of international organizations, European institutions and national decision-makers, in defending Edenred's interests and promoting its business;
- drafting messages adapted to each of these players, to preserve Edenred's solutions and programs;
- creating partnerships (and/or discussion platforms) with players involved in developing, promoting or defending policies that govern Employee Benefits solutions.

4.1.2.2 Risks related to competition law

Risk

The Group does business in highly competitive environments. When these markets are restricted to just a few players, they may sometimes give rise to anticompetitive practices. Similarly, the Group may sometimes find itself in what could be considered a dominant position, notably in the Employee Benefits market segment.

Pursuing an external growth strategy requires strict compliance with rules aimed at preventing any exchange of information with a potential acquiree before the transaction has actually been approved by the relevant authorities.

As of December 31, 2020, the Group is involved in various legal disputes related to competition law (see Note 10.3 "Claims, litigation and tax risk" to the consolidated financial statements, page 282).

Measures to manage the risk

The Legal & Regulatory Affairs Department regularly conducts training and awareness programs for executive management in the Group's subsidiaries.

4.1.2.3 Risks related to personal data protection regulations

Risk

Edenred's activities involve processing at times vast volumes of personal data from users of the Group's solutions, particularly digital solutions, as well as for other stakeholders in its business, to a lesser extent. Protecting this data is a priority for Edenred and the bedrock of stakeholder trust (see also section 5.4.2.2 "Priority issue: personal data" page 135).

In the European Union, the introduction of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) in May 2018 both harmonized personal data protection rules (thereby minimizing complexity due to regulatory differences) and strengthened these same rules, generating a vast number of compliance obligations and potential significant sanctions in the event of failure to comply.

Outside the European Union, laws and regulations to protect personal data are also being introduced and are frequently inspired by EU Regulations. This is the case, for example, in Brazil, where law no. 13.709 of August 2018 on personal data protection entered into force in August 2020.

Measures to manage the risk

The Data Protection Officer (DPO) supports the Group and its subsidiaries in the management of data related to their operations.

In the EU and a number of non-EU countries, the DPO leads and deploys a Group compliance program for personal data protection. The DPO works with a network of correspondents at the local level and throughout the subsidiaries that provide advice on the deployment of measures to ensure effective personal data protection and, by extension, compliance with personal data protection obligations. The DPO devises all of the related policies, internal guidelines and recommendations designed to ensure a consistent approach to conducting compliance-based initiatives and projects and a uniform level of regulatory compliance throughout the Group's entities.

By securing applications and data, the Digital & IT Department also plays a role in the Group's data protection regulatory compliance.

4.1.2.4 Risk related to enhanced regulatory oversight over the Group's activities via banking regulations

Risk

Two factors tend to increase the risk of enhanced regulatory oversight over our activities *via* banking regulations: (i) the increase in the number of digital solutions coupled with strong growth in the share of digital business volume, and (ii) the increasingly complex legislative and regulatory framework applicable to payment services and related solutions.

Consequently, the switch from paper vouchers to digital solutions, the launch of digital Fleet & Mobility Solutions and Corporate Payment Services together with the Group's external growth strategy in these two markets are leading to an increase in both the number of digital solutions and their contribution to overall business volume. In line with this, digital solutions accounted for 86% of the Edenred group's business volume in 2020.

At the same time, there are more and more laws and regulations governing payment services and/or e-money issuance, notably to promote financial inclusion and boost innovation in banking, but which nonetheless require the introduction of measures that are technically or financial onerous for payment solution providers.

In the European Union, Directive (EU) 2015/2366, known as the Payment Services directive 2 (PSD2), enshrines the specific features of digital Employee Benefits, explicitly excluding most of these solutions from the scope of banking and payment regulations, but nevertheless introducing an obligation to notify the local regulator for other more limited-type solutions. Outside of the European Union, countries such as Turkey, Brazil, Uruguay, Chile, the United States, Japan, India and several Southeast Asian countries have introduced legislative and regulatory requirements that apply specifically to payment services and/or e-money issuance. In most cases, the specific nature of our businesses and the ways in which these differ from payment activities are clearly recognized. However, some of these regulations affect all or part of our businesses. These regulations could require the Group to take measures that will impact:

- our organization, for example, by making it necessary to obtain a specific type of license, possibly for a dedicated entity;
- our business model, for example, by limiting commissions billable to corporate clients or partner merchants and the repayment of unused balances on expired cards; and/or
- our operations, for example, by introducing stricter rules on claims-processing deadlines and obligations to perform due diligence on corporate clients.

These legal and regulatory obstacles may limit the Group's ability to grow its businesses. The obstacles may be unexpected and require the deployment of resources and investments, which may have an adverse effect on the Group's results of operations and financial position.

Measures to manage the risk

As it does for changes in the laws and regulations applicable to solutions that qualify for specific tax treatment, the Legal & Regulatory Affairs Department implements targeted measures such as:

- continuously monitoring legal, political, social and economic developments in the Group's host countries;
- developing institutional tools that demonstrate the specific nature of Edenred's solutions vis-à-vis e-money or payment services;
- identifying the core players that are involved at the international, the European and the national level, and developing long-term contacts with them;
- participating in public debate, in order to remain a preferred contact of international organizations, European institutions and national decision-makers, in defending Edenred's interests and promoting its business model.

In some countries, specific organizations have also been set up to issue payment instruments and manage e-money or payment services under the oversight of the local supervisor in order to comply with legal and regulatory requirements applicable to certain solutions. This is notably the case in France, Italy, Brazil, the United Kingdom, Belgium, Turkey and Mexico.

4.1.2.5 Risks related to corruption, money laundering and/or terrorist financing schemes

Risk

As a French company employing over 500 people and generating total revenue in excess of €100 million, Edenred must comply with all provisions of France's Sapin 2 Act concerning transparency, the fight against corruption and the modernization of the economy.

As a stakeholder in the deployment of social policies in most of the countries in which it operates, working for both businesses and local authorities, the Group may be exposed to a risk of passive or active involvement in processes of corruption.

By their nature, the Group's businesses are relatively unexposed to the risks associated with money laundering and the financing of terrorism. Nevertheless, some specific solutions could be misused for the purpose of money laundering or even financing terrorist organizations or actions. As the transition to digital solutions accelerates and due diligence requirements applicable to regulated payment services are stepped up, additional resources are deployed.

In some countries, particularly in Latin America, subsidiaries must comply with regulations designed to combat organized crime, money-laundering and/or the financing of terrorism. This is also the case for four European subsidiaries with licenses to conduct business as e-money institutions, including one UK-based subsidiary, and Group businesses covered by e-money or payment service regulations.

Measures to manage the risk

The Legal & Regulatory Affairs Department has prepared and circulated anticorruption processes to executive management in all of the Group's subsidiaries. These processes are based on corruption risk mapping, an anticorruption Code of conduct, policies, procedures and other solutions designed to contain the risks identified, as well as a whistle-blowing procedure. In 2020, measures were deployed to strengthen the Group's existing processes based on the recommendations of the French Anti-Corruption Agency (AFA). Taking its corruption risk mapping a step further, the Group deployed a new internal whistle-blowing process in 2020 and launched an online training module on corruption risks for all employees. By end-2020, over 80% of employees with access to the platform had completed the module. As part of the Group's anticorruption processes, a new tool has been implemented to improve the efficiency and documentation of operational accounting controls.

The Group's Compliance Department assists subsidiaries to ensure compliance with the laws and regulations designed to combat organized crime, money-laundering and/or the financing of terrorism.

The four European e-money institutions reviewed and amended their anti-money-laundering and counter-terrorism-financing policies following the transposition of directives (EU) 2018/843 and 2018/1673, which amend the regulatory constraints applicable throughout the European Union.

In 2021, these measures will be bolstered by a training module for all Group employees covering the risks relating to money laundering and/or terrorist financing schemes.

4.1.3 Information systems and cybercrime risks

4.1.3.1 Information system risks

Risk

In the normal course of business, the Group and/or its service providers use a certain number of IT tools and information systems, in particular to manage digital media and for prepaid program management, notably as part of its payment operations. The main risks concern information system downtime and data availability and confidentiality, particularly for personal data. If the IT infrastructure, applications or data transmission networks were to fail, or data centre or network security were to be breached, or data were lost – accidentally or intentionally – or used for fraudulent purposes, this could disrupt the Group's business operations. This is particularly true for certain pooled applications such as transaction authorization platforms. The loss of confidential information could undermine the trust of corporate clients, resulting in a loss of business volume and exposing the Group to the risk of being ordered to pay fines or damages.

Measures to manage the risk

The Group and/or its service providers have back-up systems for these databases, located in highly secure data centres. These data centres are subject to strict administrative and technical monitoring and safeguarding procedures covering and restricting physical access to the centres themselves and the information systems they house.

In addition, the Group develops and deploys standardized information systems throughout its subsidiaries that provide the same types of product, promoting synergies and reducing risks.

Information system availability

The IT teams ensure high availability of information systems *via* the following measures, implemented at either the subsidiary or the Group level:

- infrastructure monitoring software;
- risk alert applications;
- support teams at the local, the regional and the international level that provide continuous assistance during business hours;
- on-call support staff that provide assistance outside business hours;
- a technical contingency plan setting out the process to follow in order to switch from one environment to another, when necessary.

Data protection

The IT teams ensure data protection *via* the following measures, implemented at either the subsidiary or the Group level:

- user access rights management;
- increased monitoring of privileged administrator accounts;
- intra-data centre application filtering (communication between third-party front-end applications, servers and data bases);
- data encryption, when necessary (data bases, data transmission, etc.);
- data storage encryption on laptop computers, where appropriate.

Data retention

The IT teams ensure data retention *via* the following measures, implemented at either the subsidiary or the Group level:

- regular, scheduled application environment back-ups with data retained in accordance with country-specific requirements;
- regular, scheduled database back-ups with data retained in accordance with country-specific requirements;
- secure storage spaces where users can back-up work files;
- scheduled e-mail back-ups with data retained for six months.

Protection and retention of personal data

As an employer and service provider, Edenred is particularly exposed to the rules governing the protection of personal data, such as individual identity, privacy and freedoms. Edenred has therefore established a dedicated organization, tools and a series of processes at all levels of the Group, in order to provide training, support and expertise in its operations. Edenred's information system security and data protection policies are widely circulated within the Group and are based notably on an approach that privileges the principle of privacy by design.

Program code quality management

The IT teams ensure the quality of IT programs *via* the following measures, implemented at either the subsidiary or the Group level:

- dedicated development and test environments for each application, when necessary and possible;
- dedicated User Acceptance Testing (UAT) environments;
- dedicated pre-production environments where modifications to applications are tested prior to moving to production;
- dedicated production environments.

Use of cloud computing services

The Edenred group has a corporate private cloud solution to improve its level of IT security, in particular by protecting data centres and their availability and standardizing incident management and back-ups. The cloud is accessible *via* a wide area network (WAN) which the Group has developed jointly with a leading market player.

Alongside this private cloud, in 2018 Edenred unveiled a public cloud solution that enables the Group to provide its subsidiaries with more flexible solutions, especially when deploying new applications. Since 2020, certain Group operations have migrated all of their functions over to public cloud solutions. This migration to the cloud is set to continue as part of the process of enhancing the Group's product and service quality.

These combined solutions ensure a high level of application availability and data security.

4.1.3.2 Cybercrime risks

Risk

In the normal course of business, the Edenred group and/or its service providers use a certain number of IT tools and information systems, in particular to manage digital media and for prepaid program management, notably as part of its payment operations. In the face of mounting cybercrime, the Group is exposed to the risk of cyberattacks that may impair the availability, integrity or confidentiality of confidential or sensitive data for Edenred or its clients.

Measures to manage the risk

In 2019, Edenred's Information Systems Security & Compliance Department began restructuring its Group-level cybersecurity teams to deal more effectively with cybercrime risks (see also section 5.4.2.1 "Priority issue: IT security").

Analyses and feedback from the November 21, 2019 attack were also used to reinforce protection and resilience against potential cyberattacks.

At the same time, the Group conducts internal or external audits on sensitive IT sites and infrastructure, in particular to monitor safety and improve quality if needed.

Technical measures to boost data security and detect threats

Security measures implemented by the Edenred group to prevent security incidents mainly take the form of access rights management, access traceability, surveillance of external networks (internet and darknet), external audits of sensitive services, antivirus software on workstations and servers, securing of inbound and outbound access (firewalls, proxies, WAFs, VPNs) and encryption of workstation hard drives.

Deployment of a new cybersecurity program

In 2020, the Edenred group launched a new cybersecurity program in its Information Systems Security & Compliance Department. The program aims to monitor and continually improve cybersecurity both at the subsidiary and the Group level by harnessing international IT security standards.

The program will notably cover governance, security by design, cybersecurity awareness, vulnerability and corrective patch management, IT infrastructure and computer application security, access and identity management, cybersecurity incident management and the resilience of critical IT systems.

The program will tie in with personal data protection requirements and drive a continuous and sustained improvement in IT systems security throughout the Group.

Throughout 2020, concrete improvements were made in key areas of cybersecurity, such as governance, crisis management, employee awareness, cybersecurity incident detection and management, and securing of the most critical cross-cutting IT services. This improvement program will be expanded over the coming years.

4.1.4 Group strategy and competitive environment risks

4.1.4.1 Competitive environment risks

Risk

The Group's businesses are exposed to competition from both international groups and local competitors (see section 1.1.4 "A global player dedicated to the world of work", page 24 for a description of the Group's main competitors). One or several markets may be penetrated by new entrants. These may be new companies, or existing companies that are changing their positioning in one or more markets. Competitive pressures may drive down rates in some economically fragile countries, resulting in contracts not being renewed or making it more difficult to win new contracts. If the Group is unable to effectively withstand these competitive pressures, it may lose market share or experience a decline in business or margins.

In countries where Edenred has strengthened its leading position, certain competitors or commercial partners may be tempted to claim that the Group has used this position to circumvent or distort market rules.

Measures to manage the risk

To compete effectively against the main players in its markets, the Group applies a strategy of innovation and competitive differentiation in terms of product offer, positioning, customer experience and value for money.

For example, in its Employee Benefits business, the Group has stepped up the transition from paper-based solutions to paperless versions. Edenred has also developed new services such as mobile payment and payment using application programming interfaces (APIs), which notably enable users to order from meal delivery platforms, with over 80 different partners. This differentiation strategy forms the basis of balanced and long-lasting relations with the Group's various stakeholders. In the Fleet & Mobility Solutions business line, the Group is continuing to roll out its Beyond Fuel strategy, which is aimed at offering additional services to clients by developing maintenance management, unified electronic toll and VAT recovery services for transportation companies.

In addition, to capture the potential of its existing base of clients, partner merchants and end users, the Group intends to develop customer satisfaction measurement, retention, cross-selling and monetization tools for its value-added services. Edenred is also expanding into new market segments, such as Corporate Payment Services, where it in turn is playing the role of a newcomer challenging the positions of market incumbents.

4.1.4.2 Risks associated with the acquisition strategy

Risk

The Group's strategy is based in part on external growth, mainly through acquisitions. It may not be possible to identify credible targets or to close deals at the right time and the right price.

In addition, in order to obtain approval from competition authorities for acquisitions in one or several jurisdictions, the Group may have to accept certain conditions such as a requirement to dispose of certain assets or business units.

There are a number of risks associated with acquisition strategies: (i) the business plan assumptions underlying the valuation of the target may prove to be wrong, particularly those concerning future commercial synergies and estimates of revenue growth, (ii) the Group may not be successful in integrating the acquired company, its technologies, product ranges and employees, (iii) the Group may be unable to retain all key customers of the acquired company, and (iv) the Group may have to take on additional debt to finance the acquisitions. Consequently, the benefits of current or future acquisitions may not be obtained within the forecast period or may fall short of expectations or adversely affect the Group's financial position.

Lastly, acquisitions generate risks linked to intangible asset valuation. Goodwill and other intangible assets with an indefinite useful life are tested annually for impairment. Net goodwill carried in the consolidated balance sheet at December 31, 2020 amounted to €1,457 million while net intangible assets totalled €655 million.

Measures to manage the risk

In line with its strategy, and notably its goal of maintaining an investment grade rating, the Group applies strict criteria for vetting M&A deals, particularly in relation to forecasts of recurring revenue and positive EBIT impact.

When a new business is acquired, the Group's M&A teams, liaising closely with the Strategy teams, coordinate accounting and financial, strategic and technological due diligence work involving teams from other Group functions and external consultants.

An integration plan is also prepared and the necessary resources are made available for its implementation. In particular, an Internal Audit is performed without delay, internal control principles are established and the Group's financial systems are deployed.

As regard intangible asset valuation risks, business assumptions and forecasts are prepared periodically, including a strategic plan and budget drawn up each year for each of the subsidiaries. The strategic plan and the budget are analyzed and, where necessary, an appropriate action plan is developed.

In addition, one of the objectives of the Next Frontier strategic plan is to maximize organic growth by leveraging clearly identified growth drivers, such as growth in the SME segment, which would free the Group from the need to rely on external growth alone for its development.

4.1.4.3 Risks associated with the partnership strategy and other strategic agreements

Risk

In the course of its business, the Group may use partners' technologies, IT applications or networks, particularly for digital transactions. Any disagreement concerning the renewal of any such partnerships or user licenses may have an adverse effect on the Group's business.

In addition, agreements are being implemented with clients and merchants to enable employee users to use the Group's solutions. As a result, the non-renewal of any of these partnerships may have an adverse effect on revenues from the solutions concerned.

Lastly, the Group has set up partnerships for the distribution of solutions by third parties, including an exclusive partnership agreement with Itaú Unibanco to distribute its Employee Benefits solutions in Brazil.

Measures to manage the risk

A team has been set up to manage the Group's partnerships and strategy and keep tabs on the competition. The team identifies risks upstream, sets up multiple partnerships whenever possible and identifies new partnerships to replace existing ones.

This approach can involve innovation-based agreements that strengthen the Group's positions and showcases its value proposition to clients. Distribution partnerships are structured and organized around regular exchanges between our partners, the operating entities involved and the Group. This approach helps to ensure that all parties comply with their contractual obligations over time and share the Group's best practices. Lastly, the application-based strategy deployed by the Group IT Architecture Department ensures a modular approach to acquisition of and expertise in key technologies.

4.1.5 Operational risks

The main operational risks concern business continuity and voucher fraud.

The Group is also exposed to other operational risks such as internal fraud with a lower level of criticality.

These risks are examined in detail below.

4.1.5.1 Business continuity risk

Risk

Business continuity is a key component of the Group's value proposition for its corporate clients, the employee users of its solutions, and the partner merchants that accept these solutions, together with the public authorities that deploy Employee Benefit-type programs.

The Group is exposed to two main business continuity risks: (i) the risk that its solutions cannot be used, notably in the event of inability to authorize digital solution transactions, and (ii) the risk of the Group not being able to carry on its business more generally, linked to a major failure of internal processes or essential service providers or loss of a license needed to do business in certain countries.

In 2020, the Group also had to contend with local measures taken to contain the spread of Covid-19.

Measures to manage the risk

In response to the various government measures taken to contain the spread of Covid-19, Edenred was able to deploy extensive homeworking arrangements for its employees, ensuring business continuity through its digital solutions and processes. Almost 95% of employees were able to work from home during the different lockdown periods.

The risk of inability to authorize digital solution transactions is managed by securing the continuity of transaction authorization platforms. This is made easier by centralizing all transactions on a limited number of platforms, most of which are managed by the Group.

The risk of internal failures and cybersecurity risk is managed by a series of protection measures that include internal control and audit processes, information system back-ups and deployment of disaster recovery and business continuity plans.

The risk of service provider failure is handled by tracking service provider performance and stipulating and enforcing strict contractual requirements, especially in terms of service availability and continuity.

The risk of losing a license needed to do certain business in certain countries is managed locally by executive management of the subsidiaries.

The risk of disruption to certain business lines following Brexit on December 31, 2020 was anticipated by setting up a subsidiary in Belgium. This subsidiary obtained an e-money issuer license in July 2019, enabling it to issue and distribute e-money *via* Group subsidiaries in all countries offering e-money or payment service-type solutions.

4.1.5.2 Voucher fraud risks

Risk

The Group is exposed to the risk of voucher forgery and the fraudulent use and theft of paper, card and/or paperless vouchers.

In the case of paper vouchers, risks mainly relate to the distribution of fake vouchers, voucher forgery and voucher theft. For example, the Group may be asked to accept forged or stolen vouchers presented by corporate clients for reimbursement.

In the case of cards or digital solutions, the main risks concern the fraudulent use of card details for online purchases (after the codes have been stolen using e-mail scamming and phishing or by forging cards). Forging cards or "skimming" involves stealing or obtaining card data (by hacking the information system, for example) and then copying these onto another card. The risk of actual card theft is minimal.

Combating the risk of digital solution forgery or theft requires much greater sophistication than for risks associated with paper vouchers. Cases of forgery and theft continued to be extremely rare in 2020 however, the Group continues to be attentive to new types and variation of volumes of fraud incidents, notably due to the human and economic impact of the epidemic.

Measures to manage the risk

To limit the risk, the Group continued to accelerate the migration from paper to digital solutions. This was given added impetus by the measures taken to contain the spread of Covid-19. Dematerialization and digital solutions automatically reduce exposure to the risks associated with paper solutions.

In addition, the Group has dedicated resources for integrating fraud prevention and detection mechanisms into digital solutions. Payment instrument and transaction security is being constantly improved through technological improvements, such as by equipping the cards with a smartcard chip, incorporating strong authentication solutions, stepping up security checks at payment terminals or introducing international standards, thereby helping to enhance data security.

At the same time, the Group has resources specifically dedicated to preventing fraud. Awareness raising initiatives were organized for all employees in 2020. The Group also has a policy of purchasing insurance to cover fraud risk, as explained in section 4.3.2 "Risks transferred to the insurance market", page 79.

4.2 Legal and arbitration proceedings

In the normal course of business, the Group may be involved or become involved in legal and arbitration proceedings and may be subject to tax or government audits.

Information about legal or arbitration proceedings in progress, pending or threatened that may have, or have had in the recent past, significant effects on the Group's financial position, business or results of operations is provided in Note 10.3 "Claims, litigation and tax risk" to the consolidated financial statements, page 282.

To the best of the Company's knowledge, no other governmental, legal or arbitration proceedings that may have a significant impact on the financial position of the Company and/or the Group have been initiated against the Company or any of its subsidiaries.

The method used to provide for or recognize liabilities complies with the applicable accounting standards (see section 7, Note 10.2, page 281).

Provisions for litigation are recorded on receipt by the Group of a notice of claim or summons, based on an assessment of the related risk made by the Group and its advisors. They are presented in Note 10.2 "Provisions" to the consolidated financial statements, page 281

Edenred has not entered into any material off-balance sheet commitments other than those disclosed in Note 11.5 "Off-balance sheet commitments" to the consolidated financial statements, page 286.

4.3 Transferred risks

4.3.1 Risks transferred to suppliers

The Group transfers some risk to suppliers via contract negotiations. The Group has a Purchasing Department to negotiate important supplier contracts, especially services supplied to a number of subsidiaries. This contractual risk transfer policy helps reduce the Group's residual exposure to operational as well as to information systems and cybercrime risk.

4.3.2 Risks transferred to the insurance market

Edenred transfers part of its risks onto the insurance market through business-specific insurance programs that protect its businesses and assets in all host countries. They consist of international programs that set common standards for transferring risks to insurers and optimizing cover by pool-purchasing within Group entities. To diversify counterparty risks associated with these international programs, they are spread between around a dozen top-ranking insurers, none of which covers more than 30% of the total capacity transferred to the insurance market. In 2020, 100% of the Group's programs involved insurers with an insurer financial strength rating higher than A- from Standard & Poor's.

Key insurance cover taken out by the Group and transferred to the insurance market includes:

- professional and civil liability insurance covering liability incurred by Edenred in the course of its business activities. This covers the Group's potential financial liability in the event of bodily injury, material and/or immaterial damage caused to third parties. The Group has set up an international insurance program that covers all entities throughout the world thanks to local country-specific policies;
- property and casualty and business interruption insurance covering Group assets throughout the world against accidental risks such as fire, natural disasters and other similar risks. It also covers any interruption to Edenred's business as a result of such events together with problems encountered with suppliers following an accidental event covered by a policy taken out by the Group. The individual sites purchase local cover in addition to that provided by the international program. Edenred operates close to 200 sites in 46 countries;
- anti-fraud insurance covering financial losses suffered by the Group as a result of fraud or hostile acts committed either by an employee of the insured (internal fraud) or by a third party. This policy covers paper fraud as well as payment fraud, *i.e.*, fraudulent use of cards issued by the Group. The Group has set up a worldwide insurance program rounded out by local policies taken out in countries in which a need has been identified;
- digital risk insurance covering the harm suffered/liability incurred by the Group as a result of an attack on its information systems or theft or a leak of data. This worldwide policy has been brought into line with the requirements of EU legislation to protect personal data. It is rounded out by local policies taken out in countries in which a need has been identified;
- transportation and storage insurance covering the cost of goods stolen during transportation and/or storage. Edenred has taken out an insurance policy that covers Group entities exposed to transportation risk.

The Group's international insurance program is rounded out by policies taken out in the countries in which Edenred does business. This coverage offers specific types of insurance needed in the different countries and only available locally (*e.g.*, vehicle liability insurance).

To maximize the efficiency of its insurance arsenal, the Group has chosen to self-insure against low-intensity and/or infrequent risks. Self-insurance is based around contractual deductibles and/or a reinsurance captive acquired in 2014.

- Insurance deductibles are intended to cover low-intensity risks and per-loss deductibles are adapted to each risk in line with Edenred's financial capacity to bear the amounts in question. No adjustments were made to insurance deductibles during the year;

As a primary protection measure, Edenred's reinsurance captive commits to insuring a certain amount of each risk covered. In addition to helping the Group to optimize the cost of transferring risk by retaining low-intensity and infrequent risks, the reinsurance captive also enables Edenred to address new risks that are specific to its businesses and to manage other risks in accordance with risk appetite in the insurance and reinsurance markets. In 2020, the level of risk retained by the Group reinsurance captive was reduced on transportation and on property/casualty and business interruption insurance. There was no change in the level of risk retained on other coverage.

In 2020, Edenred maintained its existing insurance coverage together with the guarantees that it has taken out on the insurance market. The Group continues to closely track the terms and conditions on offer on the insurance market.

4.4 Internal control and risk management procedures

4.4.1 Internal control definition and objectives

The Edenred group observes the highest standards in terms of internal control and financial information. Internal control is a process defined and implemented by the Board of Directors, management and employees to provide reasonable assurance regarding the achievement of objectives in the following areas:

- application of the instructions and directional guidelines fixed by Executive Management;
- compliance with the applicable laws and regulations, and adherence to the Group's corporate values;
- prevention and control of risks, particularly operational and financial risks;
- optimization of internal processes to guarantee operational efficiency and efficient use of resources;
- production of high quality, fairly stated accounting, financial and management information.

To fulfil each of these objectives, the Group has defined and implemented the main principles of internal control, based to a large extent on the Internal Control Framework defined in the report of the Committee of Sponsoring Organizations of the Treadway Commission (COSO), as last updated in 2013, and on the Internal Control Reference Framework of the French financial markets authority (Autorité des marchés financiers – AMF) and related recommendations, as last updated in 2010.

These principles are underpinned by:

- management policies that foster the development of an internal control culture and promote integrity;
- the identification and analysis of risk factors that may prevent the Group from meeting its objectives;
- an organization and procedures designed to ensure that the strategies defined by Executive Management are implemented;
- periodic reviews of control activities to seek out potential areas of improvement;
- procedures for the communication of information about internal control.

By helping to anticipate and control the risks involved in not meeting the objectives the Company has set for itself, the internal control system plays a key role in conducting and monitoring its various activities. However, internal control cannot provide absolute assurance that the Company's objectives will be met.

One of the objectives of the internal control system is therefore to anticipate and control the risks arising in the course of the Company's business, as well as the risk of errors or fraud, particularly in the areas of accounting and finance. However, as stated in the AMF's Internal Control Reference Framework, internal control procedures cannot provide absolute assurance that the Company's objectives will be met, no matter how well the system is designed or how well the procedures are applied.

The following description of the Company's internal control systems was prepared based on the AMF's Internal Control Reference Framework and its application guide.

4.4.2 Summary description of internal control procedures

The internal control system described below covers the parent company and all of its consolidated subsidiaries, which are responsible for implementing the instructions and directional guidelines fixed by Executive Management, including internal control objectives. Each subsidiary's internal control system includes both the procedures defined at the Group level and business-specific procedures that take account of the subsidiary's organization, culture, risk factors and specific operating environment. As the parent company, Edenred S.A. is responsible for ensuring that adequate internal controls exist and are applied, in particular to the accounting, financial and operating procedures of fully consolidated subsidiaries.

4.4.3 Main participants in the system of internal control

Internal control procedures are part of the policies defined by the Board of Directors and are implemented under the direct responsibility of the heads of the operating divisions and corporate functions. Internal control is everyone's responsibility, from corporate officers to front-line employees.

The main structures responsible for overseeing the internal control system are as follows:

4.4.3.1 Executive Management

In accordance with the law and the Company's bylaws, the Chairman and Chief Executive Officer represents the Company in its dealings with third parties and has the broadest powers to act on behalf of the Company in all circumstances. The situations where exercise of the Chairman and Chief Executive Officer's powers is subject to the prior approval of the Board of Directors are described in the report on corporate governance in section 6.

For the purpose of carrying out his duties, the Chairman and Chief Executive Officer has set up an Executive Committee comprising representatives from all of the operating divisions and corporate functions. The Executive Committee members are:

- Executive Vice-President, Human Resources & Corporate Social Responsibility;
- Vice-President, Communications;
- Chief Operating Officer, Americas;
- Chief Operating Officer, Fleet & Mobility Solutions;
- Chief Operating Officer, Europe, Middle East & Africa;
- Executive Vice-President, Legal & Regulatory Affairs;
- Executive Vice-President, Innovation & Asia-Pacific;
- Executive Vice-President, Marketing & Strategy;
- Executive Vice-President, Finance;
- Executive Vice-President, Global Technology.

4.4.3.2 Group Finance

The Executive Vice-President, Finance is responsible for implementing the Group's financial policies, in particular by communicating to the subsidiaries the accounting principles and standards used to prepare the consolidated financial statements.

Group Finance is organized around the following departments:

- Group Internal Audit, which includes the operating and financial Internal Audit teams, as well as information systems Internal Audit teams;
- Treasury & Financing;
- Group Accounting, responsible for overseeing the following units:
  - Group Consolidation,
  - Group Accounting of Holdings (including Edenred S.A.),
  - Group Financial Information Systems;
- Performance;
- Corporate Finance, Mergers & Acquisitions;
- Financial Communications;
- Group Tax;
- Purchasing.

Group Finance maintains regular contact with the Statutory Auditors, who audit the financial statements of the Company and the Group in accordance with the applicable laws and regulations.

Group Internal Audit & Information Systems Audit Department

Reporting to the Chief Financial Officer, the Head of Group Internal Audit has permanent access to the Chairman and Chief Executive Officer to whom he presents a report of his activities at least twice a year. The Internal Audit Department is one of the cornerstones of the internal control system, responsible for helping to develop internal control tools and standards, and for performing audits based on the multi-year audit program approved by the Board of Directors *via* the Audit and Risks Committee. The team comprises operations auditors and information systems auditors, reporting to a head of department.

Internal Audit is defined in the professional standards of the Institute of Internal Auditors (IIA) as "an independent, objective assurance and consulting activity designed to add value and improve an organization's operations and information systems." The Internal Auditors help the Group to meet its objectives by assessing its risk management, control and governance processes according to a systematic and methodical approach, and making proposals to improve their efficiency.

The Internal Audit Department's procedures are fully aligned with this definition. Its methods and procedures for reporting on its work are described in the Internal Audit Charter. This charter defines the framework for Internal Audit activities within the Group, based on the professional guidelines issued by IFACI (operations and financial audit) and ISACA (information systems audit), IIA affiliates, which require Internal Auditors to observe the highest ethical standards. It is signed by the Chairman and Chief Executive Officer, the Executive Vice-President, Finance and the head of Group Internal Audit, and approved by the Group's Audit Committee. Group Internal Audit has had IFACI Professional Certification for its professional activities since November 2017. This certification was renewed on February 2, 2021 for a three-year period.

Group Internal Audit coordinates its audit plans with the Statutory Auditors' work plans. In 2020, the Group Internal Audit team comprised the head of department and eight auditors (four operations auditors and four information systems auditors).

Treasury & Financing Department

This department is responsible for the tracking, security, transparency and efficiency of the Group's cash management and financing transactions. Its activities include:

- managing financial resources to preserve the Group's liquidity position, in agreement with the Executive Vice-President, Finance;
- managing cash positions;
- quantifying and hedging financial risks (particularly currency and interest rate risks);
- managing banking relationships;
- supporting subsidiaries in their management choices and assisting Executive Management in arranging financing for new projects.

Group Accounting Department

This department supervises and manages the Group Consolidation unit, the Group Financial Information Systems Department and the Group Accounting of Holdings Department.

It is responsible for relations with the Group's Statutory Auditors.

The role of the Group Consolidation unit consists in consolidating Group companies at the level of the ultimate parent company, Edenred S.A., which owns all of these companies either directly or indirectly. Each consolidated subsidiary produces a consolidation package in accordance with Group accounting policies and IFRSs, based on accounting data generated by their local information systems.

The Group Consolidation unit issues instructions prior to each period-end, setting out the reporting deadlines and describing any changes in standards, rules or principles that will apply for the first time. It also provides regular training on consolidation tools and standards. On receipt of the packages, the Group Consolidation unit performs the customary checks and controls before launching the consolidation process. The package reviews are an opportunity to check the accounting treatment applied to recognize and measure material, unusual and non-recurring transactions.

To help improve the quality of financial information reported by consolidated subsidiaries, the Chief Executive Officer and the Finance Director of each consolidated or non-consolidated subsidiary are required to provide the Group Consolidation team with a representation letter at each year-end, certifying that (i) the financial statements comply with Group accounting policies and principles, (ii) internal controls over the preparation and processing of the financial statements are effective, and (iii) there have been no irregularities involving employees or management. The subsidiaries' management also provide additional Human Resources information for the calculation of pension obligations, as well as comments on material events for the period and a description of any items that – individually or cumulatively – have a material impact on the understanding and measurement of the subsidiary's financial statements.

The Group Consolidation team also produces the financial statements and notes published in the Group's Annual Reports.

Group Financial Information Systems Department

The Group's financial information systems are designed to ensure the security, reliability, timeliness and traceability of financial information.

They are based on:

- a Group accounting system, to be deployed in all of the Group's subsidiaries;
- a reporting and consolidation system that covers all of the Group's operations, thereby ensuring consistency of accounting data at the Company and Group levels.

A specifically designed user manual has been prepared and issued to the employees concerned in order to guarantee that the systems are correctly used and that the information obtained is appropriate and relevant.

The Group has also set up processes to ensure the security of the financial information systems, as well as the integrity of the data involved. These include regular back-ups, programmed controls that trigger warnings in the event of incorrect data entries, and payment flow security measures.

The accounting and financial information system is regularly updated to keep pace with changes in the Group's specific needs.

The network and all centralized applications are tested periodically to ensure that they are adequately protected against intrusion risk. Regular security audits are also performed.

Performance Department

The Performance Department is made up of financial controllers and managers from Group Reporting.

The Financial Control team is tasked with ensuring that the Group deploys the right resources to achieve its growth and profitability objectives. To do this, it draws up management control guidelines and ensures that they are applied correctly in the subsidiaries. These guidelines cover both the analytical framework to be used for the Group's operating activities and the financial and non-financial indicators used to understand and manage these activities.

The Performance Department works closely with operational teams to ensure that the management framework continues to be suitable and relevant and to reflect the Group's changes and growth objectives. It also oversees the monthly performance review process with regional management and Executive Management.

In performing this duty, it draws on a team of financial controllers, each responsible for a specific region. The Performance team also works closely with Group Accounting using the same reporting tool.

The Group Reporting team is responsible for producing monthly, quarterly and annual consolidated income statements. The items in the income statements of the subsidiaries and the corporate functions are tracked and analyzed by means of operational and financial indicators, which are compared at monthly intervals with the budget and prior-year actual results. The unit also produces the data for the Group's published quarterly revenue reports.

This work serves as the basis for the preparation and transmission to the Executive Committee of management reports, supported by variance analyses and analyses of material trends identified from the subsidiaries' monthly management reporting packages.

The Executive Committee attaches considerable importance to the Group's planning process, leading to the preparation of the annual budget that rolls down the Group's strategy into operational action plans. It is the responsibility of Group Consolidation and Reporting to issue appropriate instructions and guidelines for the teams involved in preparing the budgets.

The department coordinates the planning and budget control system, which is backed by an instruction manual describing the reporting rules to be applied by all entities, as well as the budgeting and forecasting procedures.

Corporate Finance, Mergers & Acquisitions Department

Corporate Finance is responsible for all of the Group's capital transactions such as acquisitions, divestments, mergers and joint ventures. It provides expertise notably in the valuation and economic and financial structuring of acquisitions. Corporate Finance ensures compliance with Group procedures in the implementation of due diligence, negotiations with vendors and corporate finance projects. It assists the Group Accounting Department in valuation work connected with monitoring merger and acquisition transactions in the Group's consolidated financial statements (impairment testing) and goodwill allocation.

The role of Corporate Finance with respect to mergers and acquisitions involves:

- evaluating investment proposals;
- coordinating the entire acquisition process, including the acquisition audit, and centralizing the results;
- arranging the process for approving investment proposals (organizing the approval Committee meeting, presenting the proposals to the Group's Executive Committee, Executive Management and/or the Board's Commitments Committee).

Financial Communications Department

The Financial Communications Department is responsible for providing the market and the financial community with clear, accurate information about the Company's results, strategy and outlook.

It organizes and conducts ongoing dialogue with shareholders, investors and analysts through press releases, meetings, telephone conference calls, and the Company's website.

The Financial Communications Department complies strictly with the applicable regulatory framework, in particular that of the AMF, and adheres to the principle of equal treatment of all investors. With the support of the Legal & Regulatory Affairs and Group Accounting Departments, it is also responsible for reporting all regulated information (periodic and ongoing), which must meet transparency, accuracy and regularity requirements.

All financial press releases and published results are signed off by the Board of Directors and the Audit Committee prior to publication.

Group Tax Department

The Group Tax Department's responsibilities in the area of internal control are to ensure that the Group fulfils its obligations and complies with the applicable tax rules. The department's duties include:

- identifying the Group's risk exposures and implementing policies and procedures to address and attenuate tax risks;
- monitoring material tax disputes and tax audits of Group entities;
- aligning the tax practices of the various Group entities and checking with the Group's tax advisors that major transactions comply with the applicable tax laws;
- selecting tax advisors for all Edenred geographies and monitoring their services and related billings.

4.4.3.3 Legal & Regulatory Affairs Department

The Group Legal & Regulatory Affairs Department is responsible for ensuring compliance with all laws and regulations applicable to the Group in all of its host countries, protecting the Group's assets and businesses as a whole and defending its interests, as well as the professional interests of its corporate officers and employees.

It contributes to internal control in four main areas:

- drafting and updating standard contracts and contract templates for the most common transactions (purchases of IT and other goods and services, general conditions of sale, product claims, etc.), along with procedures for their use;
- making proposals to the Executive Committee regarding the rules to be applied for delegations of authority and for the distribution and protection of confidential information, introducing these rules and monitoring their correct application worldwide;
- selecting external legal advisors, monitoring their services and performance, and tracking their billings in liaison with the Management Control Department;
- transposing international standards and guidelines into Group operational requirements.

In the field of risk management, the Compliance & Risks Department, which reports to the Legal & Regulatory Affairs Department, is tasked with:

- ensuring the appropriateness of insurance coverage in relation to the risks incurred by the Group;
- mapping the Group's major risks in collaboration with the Internal Audit teams;

- monitoring the regulations mentioned in section 1.5.2 of this document (notably payment services and e-money) that may have an impact on Edenred's programs;
- providing the Group's subsidiaries with all the support they need to understand these regulations and their impact on programs and organizations.

4.4.4 Internal communication of information and procedures related to accounting and financial information

The Group ensures that relevant information is communicated in a timely manner to all persons concerned by the system of internal control so that they can perform their duties in accordance with the Group's standards. To this end, a set of procedures describing best practices and reporting processes has been circulated internally.

Internal controls over accounting and financial information are designed to provide assurance that:

- the financial information produced by consolidated subsidiaries is reliable and that the financial information published by the Group is fairly stated and complies with the true and fair view principle; and
- adequate safeguards are in place to protect against the risk of errors, inaccuracies or omissions in the Group's financial statements.

Edenred refers to the AMF's Internal Control Reference Framework and the guide to its application to internal controls over accounting and financial information.

Corporate values and principles

The Group's internal control system forms part of the corporate values expressed by the Board of Directors and Executive Management and communicated to all employees. Rules of conduct and integrity have been drawn up covering the areas of employee behaviour and relations with customers, shareholders, business partners and competitors.

Procedure manuals and accounting principles

A Finance Manual is issued to all Group Finance Departments, describing:

- the closing process for the monthly management accounts;
- the layout of the Group's charts of accounts;
- consolidation principles and accounting standards and policies used by the Group.

The manual also includes the Treasury Charter, which describes:

- cash management procedures;
- the principles to be followed concerning the holding of payment instruments and the approval of expenditures;
- the role and organization of cash pooling systems.

A presentation of International Accounting Standards/International Financial Reporting Standards has been prepared by the Group Accounting Department and made available to all Group employees concerned.

Lastly, consolidation instructions detailing the financial reporting schedule and specific adjustments to be made to the subsidiaries' local financial statements are issued every six months to the various Finance Directors and consolidation teams. They are archived on the dedicated intranet.

The subsidiaries' consolidation packages, including adjustments to comply with Group policies, are prepared by the local accounting teams using as a reference the Group Finance Manual, which describes the accounting recognition and measurement rules. The manual presents the basic concepts applied for:

- the preparation of the financial statements, such as the going concern principle;
- accounting periods;
- reliability concepts.

It is regularly updated to reflect changes in French laws and regulations governing the preparation of consolidated financial statements.

The Finance Manual also describes in detail Group principles for the recognition, measurement and presentation of the main financial statement items, including:

- descriptions and definitions of income statement items, and the consistency tests to be performed such as the tax proof;
- rules governing the recognition and presentation of balance sheet and off-balance sheet items;
- rules governing the measurement of certain items based on estimates;
- accounting and reporting principles for intra-group transactions.

Reporting procedure

The Reporting Department is responsible for overseeing the reporting procedure described in the Finance Manual. This procedure requires local teams to submit monthly reporting packages comprising an analysis of key business indicators and the main components of income, in the format prescribed by the Group. All reporting data submitted by local subsidiaries must be analyzable by nature, function and solution.

The reporting procedure is designed to provide a detailed analysis of monthly changes in consolidated financial and operating results, to support resource allocation decisions and measure the efficiency of the various organizations. Reported data are compared to the budget and to prior-year actuals to detect any emerging trends or unexplained variances.

Internal Audit reports

A draft report is prepared after each Internal Audit, setting out the auditors' findings, identified risks and related recommendations. This report is sent to the management of the audited entity, which prepares an action plan.

The final report, which includes the action plan prepared by the audited entity, is then sent to the members of the Group Executive Committee in charge of overseeing operational and financial matters for the entity concerned, as well as the corporate support functions and Executive Management.

The Audit and Risks Committee receives a half-yearly summary from the Group Internal Audit Department of the Internal Audits carried out during the period, including a status report on the annual audit plan, an assessment of the quality of internal control in the audited entities, and the Internal Auditors' main observations.

4.4.5 Identifying and analyzing risks

The Group identifies and analyzes the key risks that, if they occurred, would affect its ability to fulfil its objectives. It takes the appropriate measures to limit the probability of these risks occurring and the consequences if they do.

Identifying and assessing major risks for the Group

The Group is exposed to a number of risks in the normal course of business.

These risks, together with the related control procedures, are described in section 4 "Risk factors and management". Internal control procedures are implemented under the direct responsibility of the heads of the operating divisions and corporate functions and Group Internal Audit, and form part of an on-going process of identifying, assessing and managing risks.

The results of the analysis of non-financial risks are detailed in section 5.1.4.

Internal control self-assessments

The Group has developed internal control self-assessments, based on analyzing the internal control risks inherent in each business and identifying key control issues.

The Group places considerable emphasis on preparing, issuing and monitoring internal control self-assessment procedures. The self-assessment procedures are implemented by all Edenred entities that sell prepaid solutions in paper voucher, card and other formats. These systems are compatible with existing internal control standards and processes.

Data obtained from the internal control self-assessment procedures are centralized annually at the country level, with the assistance of the Group Internal Audit team.

Internal control risk maps are also used to plan the work performed by Group Internal Audit. These maps, which highlight issues that require priority action, are included in the relevant Internal Audit reports and are periodically presented in summary form to the Executive Committee and the Audit and Risks Committee.

Analyzing IT security risks

To round out the risk identification and assessment work conducted as part of the Group risk mapping process and the internal control self-assessment, the Group Information Systems Security & Compliance Department advises and assists Executive Management in defining its IT security policy. It is responsible for ensuring that the policy is properly implemented, applied and monitored. It also identifies, organizes, coordinates and leads all preventive and corrective security measures introduced in all of the Group's host countries.

4.4.6 Control activities

To improve control of identified risks, the Group has set up control procedures that comply with its standards and cover both operating and financial information processes.

Preparing and controlling the consolidated financial statements

The consolidated financial statements are prepared by the Group Accounting Department based on information reported by the entities' Chief Executive Officers and Finance Directors. The format of the consolidation packages is determined by the Group.

The entities are responsible for the information contained in their consolidation packages and are required to make formal representations to Group Finance about the fairness of reporting data and its conformity with Group accounting standards and policies.

The Consolidation unit carries out systematic controls of the consolidation packages submitted by the entities. A detailed schedule for reviewing the packages is prepared and sent to the employees concerned.

In connection with their audit of the consolidated financial statements, the Statutory Auditors review the consolidation packages transmitted by the entities included in the scope of their audit. Group Internal Audit also reviews from time to time the proper application of Group accounting standards and policies by the entities, and reports to Group Finance any issues identified during the review.

The consolidated financial statements are lastly examined by the Executive Vice-President, Finance prior to their review by the Audit and Risks Committee in preparation for approval by the Board of Directors.

Role of Group Internal Audit

Group Internal Audit carries out its audit assignments based on an audit program validated by the Executive Committee and the Audit and Risks Committee. The main types of assignments, as described in the Internal Audit Charter, are as follows:

- **operations and/or financial audits**, which are aimed at evaluating the reliability and effectiveness of the operating entities' internal control systems, as well as ensuring that they comply with Group standards. These audits include tracking the action plan (if any) issued following the last audit. Comparing the results of the audit with the results reported by the subsidiary during the year on the deployment of action plans serves to close the internal control loop;
- **organisational, procedural and/or specific audits**, which are aimed at helping the divisions to optimize and adapt their procedures and operating processes, notably when rolling out cross-functional projects that lead to a change in organization structures. They can also concern issues applicable to cross-cutting audits, one or more operating entities or to a particular country, function or process;
- **IT function audits**, which are performed to ensure that best practices are applied in relation to the organization and management of the audited entities' information systems. These reviews are also aimed at ensuring that the manual and automated checks in place provide an appropriate level of internal control in view of the operations covered by the applications or IT departments concerned. Lastly, they make it possible to validate the implementation of best IT project management practices.

Internal Audit plans are determined based on the internal control risk map. To ensure effective risk management, each operating entity is audited approximately every three years. The entity's contribution to the Group's operating revenue and requests from specific zone directors are also taken into account when deciding which entities should be audited. As regards the IT audit plan, the selection of auditees must take into account changes in the Group's businesses such as digitalized solutions and pooled services as well as the contribution to business volume processed by the information systems. Internal Audit successfully adapted its audit plan and procedures in 2020 to continue control operations remotely when necessary.

Measures are taken by the management of the audited entities to eliminate the identified internal control weaknesses and make any necessary improvements. The Group Internal Audit team performs a follow-up visit to check that the action plans have been duly implemented.

The head of Group Internal Audit prepares half-yearly and yearly summaries of the Internal Audits carried out by his or her teams during the year for presentation to the Executive Committee and to the Audit and Risks Committee, which checks that the department has the necessary resources and makes any observations or recommendations that it considers necessary.

4.4.7 Monitoring internal control

Internal control procedures are regularly reviewed to ensure that they are appropriate and aligned with the Group's objectives, particularly in view of the risks specific to each business and the costs of performing the controls.

The main structures responsible for overseeing the internal control system are as follows:

The Audit and Risks Committee

The Board of Directors' Internal Regulations define the Audit and Risks Committee's membership, terms of reference and procedures. The Committee is responsible for:

- ensuring that the accounting policies applied for the preparation of the financial statements of the Company and the Group are appropriate and applied consistently from one period to the next;
- monitoring the process for the preparation of financial information; and
- checking that internal reporting and control procedures provide adequate assurance concerning the reliability and completeness of financial information and the control of Group risk exposure.

It assists the Board of Directors in ensuring that the financial statements of the Company and the Group are accurate, fairly stated and reliable. To this end, the Committee makes proposals and recommendations to the Board in the areas described in section 6.1.1.12 page 171.