10

OPERATIONAL RISK

IN BRIEF

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

Operational risk RWA at end 2022

€46bn

(Amount at end 2021: €46.8bn)

Share of RWA calculated *via* the advanced approach at end 2022

97%

In line with the Group's Risk taxonomy, operational risk is one of the non-financial risks monitored by the Group. Operational risk is the risk of losses resulting from inadequacies or failures in processes, personnel or information systems, or from external events.

Societe Generale's operational risk classification is divided into eight event categories:

- commercial litigation;
- disputes with authorities;
- errors in pricing or risk evaluation including model risk;
- execution errors;
- fraud and other criminal activities;
- rogue trading;
- loss of operating resources;
- IT system interruptions.

This classification ensures consistency throughout the system and enabling cross-business analyses throughout the Group (see section 4.10.2), particularly on the following risks:

- risks related to information and communication technologies and security (cybercrime, IT systems failures, etc.);
- risks related to outsourcing of services and business continuity;
- risks related to the launch of new products/services/activities for customers;
- non-compliance risk (including legal and tax risks) represents the risk of legal, administrative or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with national or European laws, regulations, rules, related self-regulatory organisation standards, and Codes of conduct applicable to its banking activities;
- reputational risk arises from a negative perception on the part of customers, counterparties, shareholders, investors or regulators that could negatively impact the Group's ability to maintain or engage in business relationships and to sustain access to sources of financing;
- misconduct risk: risk resulting from actions (or inactions) or behavior of the Bank or its employees inconsistent with the Group's Code of Conduct, which may lead to adverse consequences for our stakeholders, or place the Bank's sustainability or reputation at risk.

The framework relating to the risks of non-compliance, reputation and inappropriate conduct is detailed in Chapter 13 *"Compliance risk, litigation"*.

10.1 ORGANISATION OF OPERATIONAL RISK MANAGEMENT

Governance

The Group operational risk management framework, other than non-compliance risks detailed in Chapter 13 *"Compliance risk, litigation"* is structured around a three-level system with the following participants:

- a first line of defence in each core Business Units/Service Units, responsible for applying the framework and putting in place controls that ensure risks are identified, analysed, measured, monitored, managed, reported and contained with the limits set by the Group-defined risk appetite;
- a second line of defence: the Operational Risk Department within the Group's Risk Division.

  In particular, the Operational Risk Department:

  - conducts a critical examination of the BU/SUs management of operational risks (including fraud risk, risks related to information systems and information security, and risks related to business continuity and crisis management),
  - sets regulations and procedures for operational risk systems and production of cross Group analyses,
  - produces risk and oversight indicators for operational risk frameworks.

  To cover the whole Group, the Operational Risk Department has a central team supported by regional hubs. The regional hubs report back to the department, providing all information necessary for a consolidated overview of the Bank's risk profile that is holistic, prospective and valid for both internal oversight purposes and regulatory reporting.

  The regional hubs are responsible for implementing the Operational Risk Division's briefs in accordance with the demands of their local regulators.

  The Operational Risk Department communicates with the first line of defence through a network of operational risk correspondents in each Business/Service Units.

  Concerning risks specifically linked to business continuity, crisis management and information, of persons and property, the Operational Risk Department carries out the critical review of the management of these risks in connection with the Group Security Division. Specifically, regarding IT risks, the Operational Risk Department carries out the critical review of the management of these risks in connection with the Resources and Digital Transformation Department.
- a third line of defence in charge of the periodic controls, carried out by the General Inspection and Audit Division.

First and Second-level control

The implementation and monitoring of the operational risk management framework is part of the Group's internal control framework:

- level 1 control is performed as part of operations within each SG Group BU/SU/entity, including managerial supervision and operational controls. This permanent control framework is supervised by the Normative Controls Library (NCL), which brings together, for the entire Group, the control objectives defined by the expertise functions, the business lines, in connection with the second lines of defence;
- level 2 control is carried out by dedicated teams in the Risk Division to carry out this mission on operational risks covering the risks specific to the various businesses (including operational risks related to credit and market risks), as well as the risks associated with purchases, communication, real estate, human resources and information system.

Risk related to security of persons and property

Protecting persons and property, and compliance with the laws and regulations governing security are major objectives for Societe Generale Group. It is the mission of the Group Security Division to manage human, organisational and technical frameworks that guarantee the smooth operational functioning of the Group in France and internationally, by reducing exposure to threats (in terms of security and safety) and reducing their impact in the event of crisis.

The security of persons and property encompasses two very specific areas:

- security is all the human, organisational and technical resources brought together to deal with technical, physical, chemical and environmental accidents that can harm people and property;
- safety is all the human, organisational and technical resources brought together to deal with spontaneous or thoughtful acts aimed at harming or impairing with the aim of psychic or/and financial profit.

The management of all these risks is based on operational risk systems and the second line of defence is provided by the Risk Department.

Risks related to information and communication technology (ICT) and security risks

Given the importance for the Group of its information system and the data it conveys and the continuous increase in the cybercriminal threat, the risks related to information and communication technologies (ICT) and to security are major for Societe Generale. Their supervision, integrated into the general operational risk management system, is steered as the first line of defence by a dedicated area of expertise (Information and Information Systems Security – ISS) and the second line of defence is provided by the Risk Department. They are subject to specific monitoring by the management bodies through sessions dedicated to Group governance (Risk Committee, CORISQ, CCCIG, DTCO) and a quarterly dashboard which presents the risk situation and action plans on the main information and communication technologies risks.

The Department Security of the Group, housed within the General Secretariat, is responsible for protecting information. The information provided by customers, employees and also the collective knowledge and know-how of the bank constitute Societe Generale's most valuable information resources. To this end, it is necessary to put in place the human, organisational and technical mechanisms which make it possible to protect the information and ensure that it is handled, disseminated, shared by only the people who need to know.

The person in charge of risks related to information and communication technologies (ICT) and security of information systems is housed at the Corporate Resources and Digital Transformation Division. Under the functional authority of the Director of Group Security, he recommends the strategy to protect digital information and heads up the IT Security Department. The IT security framework is aligned with the market standards (NIST, ISO 27002), and implemented in each Business/Service Unit.

Risk management associated with cybercrime is carried out through the tri-annual Information Systems Security (ISS) master plan.

In order to take into account the evolution of the threat, in particular that related to ransomware, and in line with the Group strategy, the ISS 2021-2023 master plan is structured, with a budget of EUR 650 million over the period 2021-2023, around two pillars that guide actions by 2023:

- protect the data of our customers and our ability to operate the banking services, by integrating the threats, the requirements of the regulators, and the need to support the Business Units and Service Units in their digital transformation and the evolution of uses that accompanies it. A risk-based approach allows us to concentrate our efforts on the most critical elements and data, in connection with the work of the Security Department cited above. We are preparing to manage a major cyber crisis by improving in particular our detection capacity, our ability to control our IT links with our partners and subsidiaries, and our ability to rebuild the information system;
- increase our operational efficiency by gaining overall consistency, and by increasing our protections and our ability to react. In particular by developing the management of the Cyber Security Department, by optimising our processes and our tools to be able to deploy new protections at constant cost. Finally, by working on the management of human resources in the filiere, in particular on the development of skills and networks of expertise.

At the operational level, the Group relies on a CERT (Computer Emergency Response Team) unit in charge of incident management, security watch and the fight against cybercrime. This team uses multiple sources of information and monitoring, both internal and external. Since 2018, this unit has also been strengthened by the establishment of an internal Red Team whose main tasks are to assess the effectiveness of the security systems deployed and to test the detection and reaction capabilities of the defence teams (Blue Teams) during an exercise simulating a real attack. The services of the Red Team enable the Group to gain a better understanding of the weaknesses in the security of the Societe Generale information system, to help in the implementation of global improvement strategies, and also to train cybersecurity defence teams. CERT works closely with the Security Operation Center (SOC), which is in charge of detecting security events and processing them.

A team at the Resources and Digital Transformation Department is in charge of the consistency of the implementation of operational risk management systems and their consolidation for IT processes. The main tasks of the team are as follows:

- identify and evaluate the major IT risks for the Group, including extreme risk scenarios (*e.g.* cyberattack, failure of a provider), to enable the Bank to improve its knowledge of its risks, be better prepared for extreme risk scenarios and better align their investments with their IT risks;
- produce the indicators that feed the IT risks monitoring dashboard, intended for management bodies and Information Systems Directors. They are reviewed regularly with the second line of defence in order to remain aligned with the IS and SSI strategy and their objectives;
- more generally, ensure the quality and reliability of all devices addressing IT operational risks. Particular attention is paid to the permanent control system for its IT risks, which is based on the definition of normative IT and security controls and the support of the Group in the deployment of managerial supervision on this topic. As part of the "PCT" program to transform permanent control, the normative controls were reviewed, *i.e.* around thirty controls on IS/SSI subjects. The IT Department monitors the deployment of these controls across the Group, the progress of which is aligned with the objectives set by the Group.

In terms of awareness, a multilingual online training module on information security is mandatory for all internal Group staff and for all service providers who use or access our information system. It was updated in early 2020 in order to incorporate changes to the new Group Information Security Policy. At the end of August 2021, 98% of Societe Generale Group employees who were notified of the training module had performed it.

Risks related to fraud and non-authorized market activities (rogue trading)

The supervision of fraud risk, whether internal or external, is integrated into the general operational risk management framework which allows the identification, assessment, mitigation and monitoring of the risk, whether it is potential or actual.

It is steered in the first line of defense by dedicated expert teams dedicated to fraud risks management in addition to the teams in charge of operational risk management specific to each of the banking businesses. These teams are in charge of the definition and operational implementation of the means of raising awareness, preventing, detecting and dealing with frauds. The second line of defense is provided by the Operational Risks Department with a fraud risk manager. The second line defines and verifies compliance with the principles of fraud risk management in conjunction with the first line teams, and ensures that the appropriate governance is in place.

Finally, the teams, whether they are in the first or second line of defense, work jointly with teams of experts in charge of information security, the fight against cyber crime, customer knowledge, the fight against corruption and money laundering. Likewise, the teams work closely with the teams in charge of credit risk and market risk. The sharing of information contributes to the identification and increased responsiveness in the presence of a situation of proven fraud or weak signals. This active collaboration makes it possible to initiate investigative measures, blocking attempted fraud or initiating the recovery of funds or the activation of guarantees, associated insurance in the event of successful fraud.

10.2 OPERATIONAL RISK MONITORING PROCESS

The Group's main frameworks for controlling operational risks are as follows:

- collection and analysis of internal operational losses and significant incidents that do not have a financial impact;
- risk and control self-assessment (RCSA);
- oversight of key risk indicators (KRI);
- development of scenario analyses;
- analysis of external losses;
- framework of new products and services;
- management of outsourced services;
- crisis management and business continuity;
- management of risks related to information and communication technologies.

Collection of internal operational losses and significant incidents without any financial impact

Internal losses and significant incidents without any financial impact are compiled throughout the Group. The process:

- monitors the cost of operational risks as they have materialised in the Group and establishes a historical data base for modelling the calculation of capital to be allocated to operational risk;
- learns from past events to minimize future losses.

Analysis of external losses

External losses are operational losses data shared within the banking sector. These external data include information on the amount of actual losses, the importance of the activity at the origin of these losses, the causes and circumstances and any additional information that could be used by other establishments to assess the relevance of the event as far as they are concerned and enrich the identification and assessment of the Group's operational risk.

Risk and control self-assessment

Under the Risk and Control Self-Assessment (RCSA), each manager assesses the exposure to operational risks of its activities within its scope of responsibility, in order to improve their management.

The method defined by the Group consists of taking a homogeneous approach to identifying and evaluating operational risks and frameworks to control these risks, in order to guarantee consistency of results at Group level. It is based notably on Group repositories of activities and risks in order to facilitate a comprehensive assessment.

The objectives are as follows:

- identifying and assessing the major operational risks (in average amount and frequency of potential loss) to which each activity is exposed (the intrinsic risks, *i.e.* those inherent in the nature of an activity, while disregarding prevention and control systems). Where necessary, risk mapping established by the functions (*e.g.* Compliance, Information Systems Security, etc.) contributes to this assessment of intrinsic risks;
- assessing the quality of major risk prevention and mitigation measures;
- assessing the risk exposure of each activity that remains once the risk prevention and mitigation measures are taken into account (the "residual risk"), while disregarding insurance coverage;
- remedying any shortcomings in the prevention and control systems, by implementing corrective action plans and defining key risk indicators; if necessary, in the absence of an action plan, risk acceptance will be formally validated by the appropriate hierarchical level;
- adapting the risk insurance strategy, if necessary.

The exercise includes, in particular, risks of non-compliance, reputational risk, tax risks, accounting risks, risks related to information systems and their security, as well as those related to human resources.

Key risk indicators

Key risk indicators (KRIs) supplement the overall operational risk management system by providing a dynamic view (warning system) of changes in business risk profiles.

Their follow-up provides managers of entities with a regular measure of improvements or deteriorations in the risk and the environment of prevention and control of activities within their scope of responsibility.

KRIs help BU/SU/Entities and the Senior Management proactively and prospectively manage their risks, taking into account their tolerance and risk appetite.

An analysis of Group-level KRIs and losses is presented to the Group's Executive Committee on a quarterly basis in a specific dashboard.

Analyses of scenarios

The analyses of scenarios serve two purposes: informing the Group of potential significant areas of risk and contributing to the calculation of the capital required to cover operational risks.

These analyses make it possible to build an expert opinion on a distribution of losses for each operational risk category and thus to measure the exposure to potential losses in scenarios of very severe severity, which can be included in the calculation of the prudential capital requirements.

In practice, various scenarios are reviewed by experts who gauge the severity and frequency of the potential impacts for the Group by factoring in internal and external loss data as well as the internal framework (controls and prevention systems) and the external environment (regulatory, business, etc.). Analyzes are carried out either at Group level (transversal scenarios) or at business level.

Governance is established in particular, to:

- allow the approval of the annual scenarios update program by Senior Management through the Group Risk Committee (CORISQ);
- allow the approval of the scenarios by the businesses (for example during the internal control coordination Committees of the BU and SU concerned or during *ad hoc* meetings) and a challenge of scenario analyses by LoD2;
- conduct an overall review of the Group's risk hierarchy and of the suitability of the scenarios through CORISQ.

New product Committees

Each division submits its plans for a new product and services to the New Product Committee. The Committee, jointly coordinated by a representative of the Group Risk Division and a representative of the relevant businesses division, is a decision-making body which decides the production and marketing conditions of new products and services to customers.

The Committee aims to ensure that, before any product launch or service, or before any relevant changes on an existing product or service, all types of induced risks (among them, credit, market, liquidity and refinancing, country, operational, legal, accounting, tax, financial, information systems risks as well as the risks of non-compliance, reputation, protection of personal data, corporate social and environmental responsibility risks, etc.) have been identified, assessed and, if necessary, subjected to mitigation measures allowing the acceptance of residual risks.

Management of outsourced services

Some banking services are outsourced outside the Group or within the Group (*e.g.* in our shared service centers). These two subcontracting channels are supervised in a manner adapted to the risks they induce.

The management framework for outsourced services ensures that the operational risk linked to outsourcing is controlled, and that the conditions set by the Group's approval are respected.

The objectives are as follows:

- decide on outsourcing with knowledge of the risks taken; the entity remains fully responsible for the risks of the outsourced activity;
- monitor outsourced services until they are closed, ensuring that operational risks are controlled;
- map the Group's outsourcing activities with an identification of the activities and BUs concerned in order to prevent excessive concentrations on certain service providers.

Crisis management and business continuity

Crisis management and business continuity measures aim to minimize as much as possible the impact of potential disasters on customers, staff, activities or infrastructures, and thus to preserve the Group's reputation and image as well as its financial strength.

Business continuity is managed by developing in each Societe Generale Group entity, organisations, procedures and resources that can deal with natural or accidental damage, or acts of deliberate harm, with a view to protect their personnel, assets and activities and to allow the provision of essential services to continue, if necessary, temporarily in reduced form, then restoring service to normal.

10.3 OPERATIONAL RISK MEASUREMENT

Since 2004, Societe Generale has used the Advanced Measurement Approach (AMA) allowed by the Capital Requirements Directive to measure operational risk. This approach, implemented across the main Group entities, notably makes it possible to:

- identify the businesses that have the greatest risk exposures;
- identify the types of risk that have the greatest impact on the Group's risk profile and overall capital requirements;
- enhance the Group's management of operational risks.

Operational risk modeling

The statistical method used by the Group for operational risk modeling is based on the Loss Distribution Approach (LDA) for AMA internal model.

Under this approach, operational risks are modeled using segments, each segment representing a type of risk and a Group core business. The frequency and severity of operational risks, based on past internal losses, external losses, the internal and external environment, and scenario analyses, are estimated and the distribution of annual losses is calculated for each segment. This approach is supplemented by cross-business scenario analyses that measure cross-business risks for core businesses, such as cybercriminality and the flooding of the river Seine.

Aside from the individual risks associated with each segment or cross-business scenario analysis, the model takes into account the diversification between the various types of risk and the core businesses, dependency effects between extreme risks as well as the effect of insurance policies taken out by the Group.

The Group's regulatory capital requirements for operational risks within the scope covered by the (AMA) internal model are then defined as the 99.9% quantile of the Group's annual loss distribution.

For some Group entities, notably in retail banking activities abroad, the standard method is applied: the calculation of capital requirements is defined as the average over the last three years of a financial aggregate based on the Product Net Banking multiplied by factors defined by the regulator and corresponding to each category of activity. To make the calculation, all of the Group's business lines are broken down into the eight regulatory activities.

Societe Generale's total capital requirements for operational risks were EUR 3.7 billion at the end of 2022, representing EUR 46 billion in risk-weighted assets. This assessment includes the capital requirement of AMA and Standard perimeters.

Insurance cover in risk modeling

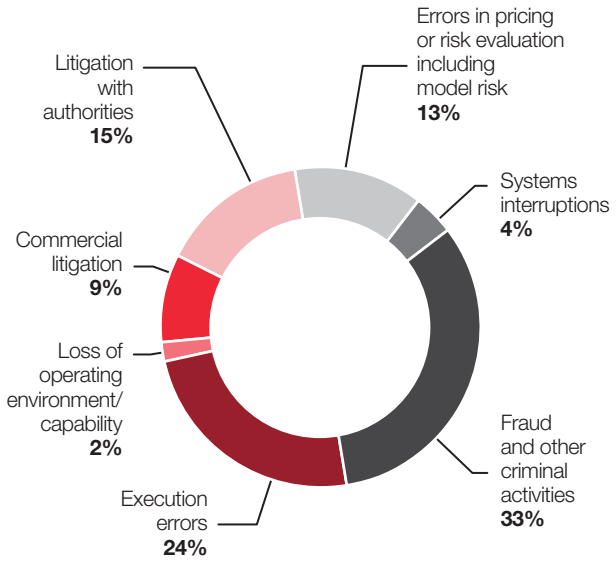
In accordance with regulations, Societe Generale incorporates risk cover provided by insurance policies when calculating regulatory capital requirements for operational risks, within the limit of 20% of said requirements. These insurance policies cover part of the Group's major risks, *i.e.* civil liability, fraud, fire and theft, as well as systems interruptions.

Risk reduction through insurance policies resulted in a 6.5% decrease in total capital requirements for operational risks.

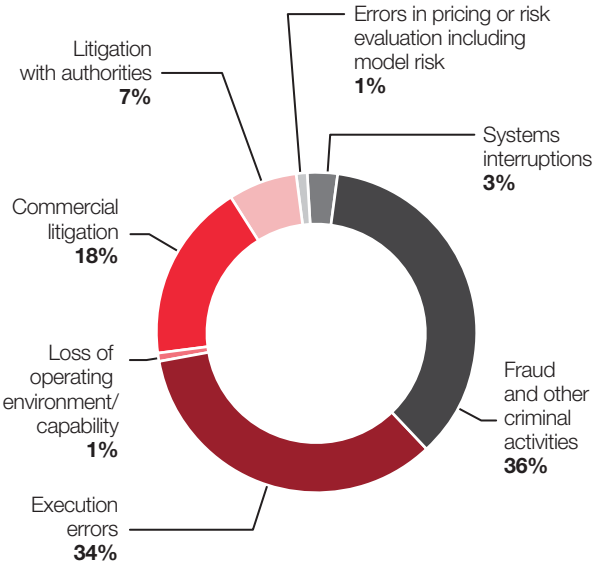
Quantitative data

The following charts break down operating losses by risk category for the 2018-2022 period.

OPERATIONAL RISK LOSSES: BREAKDOWN BY SOCIETE GENERALE RISK EVENT TYPE - AMOUNTS



OPERATIONAL RISK LOSSES: BREAKDOWN BY SOCIETE GENERALE RISK EVENT TYPE - NUMBER OF EVENTS



Over the past five years, Societe Generale's operational risks were concentrated on average on five types, accounting for 94% of the Group's total operating losses:

- fraud and other criminal activities represented 33% of the amount of operating losses over the period. They are mainly composed of external frauds on financing files (falsified financial statements by the client, theft or misappropriation of collateral/guarantees, etc.), fraud on manual means of payment (cash, transfer and cheque) and supplier fraud on financed equipment; slight increase in 2022 due in particular to regularizations on old external fraud files;
- execution errors represented 24% of total operational losses, thereby constituting the second leading cause of loss for the Group; The decrease trend that began in 2021, continues in 2022 thanks to the proper execution of the remediation plans;
- litigation with authorities, the third largest category, represented 15% of the Group's operational losses over the period; the net amount of provisions for litigation has decreased in 2022 compared to 2021;
- pricing or risk assessment errors, including model risk, represent 13% of the total amount of losses. The main cases concern the pricing and ALM models;
- commercial disputes represented 9% of total Group operating losses.

The other categories of Group operational risk (activities not authorised on the markets, system interruptions, loss of operating environment/capability) were still relatively insignificant, representing 6% of the Group's losses on average over the 2018 to 2022 period.

10.4 RISK-WEIGHTED ASSETS AND CAPITAL REQUIREMENTS

Societe Generale's capital requirements for operational risk are mainly calculated using the Advanced Measurement Approach (AMA) *via* its internal model (97% in 2022).

The total amount of RWA decreased in 2022 (EUR -0.8 billion, *i.e.* -1.7%) mainly due to the sale of Russian business.

The following table breaks down the Group's risk-weighted assets and the corresponding capital requirements at 31 December 2022.

TABLE 97: WEIGHTED EXPOSURES AND CAPITAL REQUIREMENTS FOR OPERATIONAL RISK BY APPROACH

	31.12.2022				
(In EURm)	Relevant indicator			Own funds requirements	Risk-weighted assets
Banking activities	**31.12.2020**	**31.12.2021**	**31.12.2022**		
Banking activities subject to basic indicator approach (BIA)	0	0	0	0	0
Banking activities subject to standardised (TSA)/alternative standardised (ASA) approaches	1,184	1,337	1,245	103	1,290
Subject to TSA	*1,184*	*1,337*	*1,245*		
Subject to ASA	0	0	0		
Banking activities subject to advanced measurement approaches AMA	21,964	23,980	27,186	3,579	44,733

	31.12.2021				
(In EURm)	Relevant indicator			Own funds requirements	Risk-weighted assets
Banking activities	**31.12.2019**	**31.12.2020**	**31.12.2021**		
Banking activities subject to basic indicator approach (BIA)	-	-	-	-	-
Banking activities subject to standardised (TSA)/alternative standardised (ASA) approaches	1,365	1,437	1,481	193	2,412
Subject to TSA	*1,365*	*1,437*	*1,481*		
Subject to ASA	-	-	-		
Banking activities subject to advanced measurement approaches AMA	23,643	21,964	23,980	3,552	44,394

(1) Historical data including the updates, reflecting some evolutions in the scope of entities, which occurred across the year.

10.5 OPERATIONAL RISK INSURANCE

General policy

Since 1993, Societe Generale has implemented a global policy of hedging Group operational risks through insurance.

This consists in searching the market for the most extensive cover available for the risks incurred and enabling all entities to benefit from such cover wherever possible. Policies are taken out with leading insurers. Where required by local legislation, local policies are taken out, which are then reinsured by insurers that are part of the global program.

In addition, special insurance policies may be taken out by entities that perform specific activities.

A Group internal reinsurance company intervenes in several policies in order to pool high-frequency, low-level risks between entities. This approach contributes to the improvement of the Group's knowledge and management of its risks.

Description of main general risk coverage

Buildings and their contents, including IT equipment, are insured at their replacement value. The guarantee covering acts of terrorism abroad has been renewed.

Liability other than professional liability (*i.e.* relating to operations, Chief Executive Officers and Directors, etc.) are covered. The amounts insured vary from country to country, according to operating requirements.

Description of main risks arising from operations

Insurance is only one of the measures used to offset the consequences of the risks inherent in the Group's activity. It complements the Group's risk management policy.

THEFT/FRAUD

These risks are included in the "Banker's Blanket Bond" policy that insures all the Group's financial activities around the world.

Internal fraud (committed by an employee or by a third party acting with the aid of an employee) and external fraud (committed by a third party acting alone), with the intent to obtain illicit personal gain or to harm the Group, are covered.

PROFESSIONAL LIABILITY

The consequences of any legal on staff or managers in the Group's professional activities are insured under a global policy.

CYBERATTACKS

A cyber risk insurance policy has been taken out amid an environment not specific to the banking sector which is seeing a rapid development of new forms of crime mainly involving data theft or the compromise or destruction of computer systems.