

# • the Compliance

## **The Compliance function within BNP Paribas**

The Compliance function was established in December 2004, in anticipation of Regulation 97-02 relating to internal controls in the banking industry. Its purpose is to control risks in respect of professional ethics and in 2006 the Group made concerted efforts to reinforce the function's operating procedures. Risk management is key to BNP Paribas' organisation, management and strategy, and the management of risks that could endanger the Bank's compliance is of particular significance. The Group defines compliance as "adhering to laws and regulations, professional and ethical standards and practices, the guidelines of the Board of Directors and the instructions of Group Executive Management". It encompasses protection of the Group's reputation and the implementation of its guiding principles, respect for

the integrity of the markets and the primacy of clients' interests, professional ethics, and the fight against money laundering, terrorism and corruption. It meets criteria of exhaustiveness and universality and the same high standards are required regardless of the entity or business, in France or abroad, by applying the "best interests" principle, which stipulates that the most stringent of the regulations laid down by the laws of the various countries and the Group's own directives and procedures will be applied.

### **Dedicated teams...**

The compliance control mechanism, which is an integral part of internal control, comes under the responsibility of a dedicated Group Compliance function. Under the direct control of the Chief Executive Officer, this function is managed by a member of the Executive Committee, who is also responsible for permanent internal control

as regards the regulator and who coordinates the workings of the internal control mechanism. The Compliance function, whose responsibilities are laid down by the Internal Control Charter and the Compliance Charter, comprises both a central team and local teams. The central team oversees the running of the function and sets the standards and procedures applicable in the Group. The local teams in the divisions, business lines, functions, subsidiaries and branches, who are in direct contact with transactions, represented 614 people as at 31 December 2006, i.e., over 90% of the function's staff. These employees hold high levels of responsibility, under the joint authority of the manager of the function and the entity's operational manager, pursuant to the principle that operational staff are at the front-line of risk management. In 2006, BNL's compliance teams adopted BNP Paribas' compliance standards.

## • the Compliance

### > ...Updating procedures...

The Compliance function, in its capacity as provider of compliance control and advice, is mainly responsible for ensuring general compliance procedures and assisting Group entities with problems of all kinds that they may encounter in this area. In 2006, several major policies were updated at Group level, notably:

- A directive on reputation risk management, which sets out the best ways for the Group to protect its reputation among its customers, counterparties, regulators, and all parties implicated in upholding the Group's reputation;
- A directive on conflict of interest management, which concerns protecting clients' interests, the Group's reputation, and the strengthening of regulatory requirements, in particular in light of the European Markets in Financial Instruments Directive (MiFID), which will come into force in late 2007;

- A new Group directive on the procedures for authorising non-recurring directives, new products and new activities details the extent to which local compliance teams may intervene as regards managing risks that may harm the Group's reputation, or the unsuitability of products to customers' needs. The tools for detecting and managing non-compliance risk situations are playing an increasingly central role, in particular the ethics alert mechanism, operational in France and certain international sites. In accordance with the requirements of banking and finance regulations and pursuant to data protection and banking secrecy laws, this mechanism ensures the confidentiality of transactions. It only deals with compliance-related issues, i.e., anything that may harm the Bank, either in terms of its reputation or its compliance with laws and procedures, market integrity, and respect for the primacy of customers' interests.

### > ... and managing the financial security mechanism

Within the Compliance function, the financial security teams coordinate the prevention of money laundering, the fight against corruption and terrorism financing, and the application of financial embargoes, a source of significant obligations for financial intermediaries. They deal with the reporting of suspicions on the French market and set standards in specialist domains such as "Know Your Customer" (KYC), with regard to the prevention of money laundering. The duty of care principle is a legal obligation for financial institutions, which extends to all their core businesses. A circular distributed in 2006 enhances the mechanism regarding "Know Your Customer" and acceptance of third parties, third parties covering non-group asset managers, referral agents, etc. It also describes the use of IT tools aimed at identifying clients that may pose a risk and strengthening transaction monitoring.

## • the Compliance

The international situation has led the authorities to put in place sanctions in respect of certain countries or goods, by imposing financial embargos. Instructions relating to the application of these embargos lay down imperative guidelines for detecting and dealing with transactions by customers targeted by these measures, in accordance with the legislation in force.

BNP Paribas has set itself the goal of limiting and strictly coordinating its presence in countries qualified as tax havens, in order to improve its control of unforeseeable administrative complications and any risk to its reputation that could occur as a result. Procedures and rules of conduct define the countries involved, the control regulations for companies operating in these countries and the compliance and financial security mechanisms. In accordance with the “best interests” principle, Group regulations

on combating money laundering, corruption and terrorism financing, as well as on compliance with embargos, apply to entities domiciled in tax havens, even if local regulations are less strict.

New IT control tools were developed in 2006, representing a major investment for the Group. These include a database of politically exposed persons (Lynx); a system that automatically checks customer lists against lists of sanctions and politically exposed persons (Sun); a reference system for sanction lists (Regliss); an anti-terrorism filter and embargo application system (Shine); a tool for analysing the functioning of accounts to detect money laundering operations (Iris); and a new tool for managing the reporting of suspicions (Sysfact).

Compliance training, in particular as regards the fight against money laundering, is one of the function’s main responsibilities. In 2006, this training was provided to almost 63,000 employees, a 45% increase on 2005. An e-learning module to raise awareness regarding compliance was developed centrally. Two new modules were created for the detection of market abuse (insider trading and stock manipulation) and the implementation of the MiFID, which contains important compliance-related provisions which should improve the execution of transactions, the adaptation of products to clients’ needs, the provision of information, and conflict-of-interest management.

### Business continuity

Business continuity is an area of constant concern for the Group. In the 1980s, both BNP and Paribas implemented information system security procedures. To address outside events, changes in regulations and increased pressure from customers, these procedures are continually upgraded in all of the Bank's businesses and territories. In 2006, Group-wide coordination became part of a global business continuity approach and helped to provide a clearer cross-functional perspective across the fast-growing Group. Numerous local initiatives were also implemented, including the creation of a dedicated site in New York, and improved coordination of business continuity and disaster recovery plans in London.

#### > Organisation of continuity efforts

Business continuity is organised around three main pillars.

- Group Compliance defines the standard business continuity guidelines applicable across the Group;
- The Group Operating Efficiency function develops strategy, methodology and rules and regulations based on defined guidelines, acts in accordance with the principles of consistency and oversees the implementation of the strategy;
- The entities draw up, implement and test their continuity plan.

A dedicated Group Security team has also been set up to coordinate the implementation of a proactive and effective crisis management policy throughout the Group.

#### > Operational management of business continuity plans

All BNP Paribas entities are directly responsible for identifying their continuity imperatives and

drawing up an appropriate action plan (business continuity plan), testing the effectiveness of the plan on a regular basis, and defining and implementing specific crisis management procedures. These responsibilities are part of a standard Group methodology designed to ensure that the continuity plan is effective. This methodology consists of four phases:

**Phase 1 – preliminary steps:** these include identifying continuity solutions, in particular disaster recovery plans and user business continuity plans in relation to risks such as power cuts, fire, floods, earthquakes, landslides, terrorist attacks or strikes that would lead to employees being unable to access the Group's premises or process transactions; designating key players; assessing the regulatory requirements, including those applicable to outsourced activities; and identifying critical business components: key employees, systems, applications and data, as well as logistics (availability, access, security, utility and supplies).

## • the Compliance

**Phase 2 – Analysing and reporting continuity imperatives:** each entity defines the critical components necessary to continue working in an emergency: strategic activities and their financial, commercial, regulatory or reputational impacts are listed, prioritised and validated. The maximum periods of allowable interruption are assessed, validated and reviewed on a regular basis. Strategic databases and tools are listed, prioritised and validated, in particular constraints in system usage mode and data access, together with the maximum allowable data losses. Logistics and communication tools for strategic businesses are identified, and conditions ensuring employee and data security (authentication, authorisation management, back-ups and data warehousing) are defined.

**Phase 3 – Launch and implementation of business continuity strategies:** procedures are drawn up for triggering continuity solutions in each crisis situation. Organisational, functional and technical procedures are documented and updated at least once a year.

**Phase 4 – Continuous review:** The business continuity plans are regularly tested and the corresponding documentation is updated in line with changes in the technical or regulatory environment.

Over the past few years, BNP Paribas has significantly increased its resilience, even though it may be difficult to protect the Group against every eventuality. Business continuity is not only a requirement imposed by banking regulations, it is also a major focus of attention for the Group, which seeks to offer its clients, shareholders and employees a commitment of the Bank's strength and resilience in an increasingly complex and volatile environment where tensions may be experienced more frequently. This imperative is reflected in the business continuity plans in place, which help improve the performance of operational risk control and crisis management systems, while ensuring that resources are allocated in an efficient manner.