**Operational Risk Disclosure**

Operational risk is the risk of incurring a loss due to inadequate or failed internal processes, or due to external events, whether deliberate, accidental or natural occurrences. Management of operational risk is based on an analysis of the “cause – event – effect” chain.

Internal processes giving rise to operational risk may involve employees and/or IT systems. External events include, but are not limited to floods, fire, earthquakes and terrorist attacks. Credit or market events such as default or fluctuations in value do not fall within the scope of operational risk.

Operational risk encompasses fraud, human resources risks, legal risks, non-compliance risks, tax risks, information system risks, conduct risks (risks related to the provision of inappropriate financial services), risk related to failures in operating processes, including loan procedures or model risks, as well as any potential financial implications resulting from the management of reputation risk.

**Operational Risk Identification & Overall Strategy**

The BNP Paribas general policy regarding operational risk is to have the operating management be accountable for managing the risks generated by the activity under their responsibility. RISK, as an independent control function, acts as a second line of defense, defining the global framework, challenging output from risk and control self-assessments, testing the risk mitigation framework and independently reporting risks to the Senior Management.

This principle presupposes that the managers identify and assess their operational risks, formalize and disclose them transparently, and take measures to prevent and correct any vulnerability identified in this manner, while doing so in consistency with the risk tolerance defined by the BNP Paribas Group and its translation throughout the entities for which they are responsible.

The major steps of the risk and control self-assessment (RCSA) exercise for operational risk are:

* Identification, analysis and the assessment of the underlying risks.
* Analysis of the actual functioning of the control system and of dynamic risk indicators,
* Residual risk, which provides an assessment of the risk having taken into account the actual functioning of the control framework and its results in terms of risks at a given point of time.

The RCSA exercise should be conducted on a regular basis, or more frequently should it be needed. The most material risks identified then need to be analyzed more deeply for risk management purposes.

On a yearly basis, BNP Paribas Group runs a formal process of reporting of key attention points in terms of operational risk through a bottom up approach, each level being subject to a formal sign-off from the Head of the entity concerned. This exercise is made from the RCSA outputs, analysis of actual incidents, results from controls & key risks indicators and output from audits assignments (internal audits, external audits, supervisory reviews …). It is challenged by RISK as the independent control function in charge of operational risk and permanent control framework.

### Operational Risk Strategy

The BNP Paribas Group aims at protecting its customers, its staff and its shareholders from operational risk either by avoidance, mitigation or transfer. It strives to contain operational risk, insofar as possible, to acceptable levels. The BNP Paribas Group develops a comprehensive risk and control management framework covering risk awareness and culture, risk identification and anticipation, risk mitigation techniques, risk monitoring and governance.

The internal control framework with respect to operational risk is aligned to the three lines of defense’s model:

* A first line of defense under the responsibility of the teams in charge of the operational implementation of the processes and that builds on the skills referred to as Operational Permanent Control (OPC),
* A second line of defense consisting of independent permanent control functions, and in particular Operational Risk and Control (Risk ORC) teams,
* A third line of defense ensured, under a mission of periodical control, by the Internal Audit.

Internal audit is regularly reviewing both the way the second line of defense operates and how the operational risk and permanent control framework works with the first line of defense.