

activities. The definition does not include strategic or reputational risks.<sup>8</sup>

- **Operational risk loss:** The financial impact associated with an operational event that is recorded in the institution's financial statements consistent with Generally Accepted Accounting Principles (GAAP). Financial impact includes all out-of-pocket expenses associated with an operational event but does not include opportunity costs, foregone revenue, or costs related to investment programs implemented to prevent subsequent operational risk losses. Operational risk losses are characterized by seven event factors associated with:

- i. **Internal fraud:** An act of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involve at least one internal party.

- ii. **External fraud:** An act of a type intended to defraud, misappropriate property or circumvent the law, by a third party.

- iii. **Employment practices and workplace safety:** An act inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.

- iv. **Clients, products, and business practices:** An unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.

- v. **Damage to physical assets:** The loss or damage to physical assets from natural disaster or other events.

- vi. **Business disruption and system failures:** Disruption of business or system failures.

- vii. **Execution, delivery, and process management:** Failed transaction processing or process management, from relations with trade counterparties and vendors.

- **Operational risk exposure:** An estimate of the potential operational losses that the banking institution faces at a soundness standard consistent with a 99.9 per cent confidence level over a one-year period. The institution will multiply the exposure by 12.5 to obtain risk-weighted assets for operational risk; this is added to the risk-weighted assets for credit and market risk to arrive at the denominator of the regulatory capital ratio.

- **Business environment and internal control factor assessments:** The range of tools that provide a meaningful

assessment of the level and trends in operational risk across the institution. While the institution may use multiple tools in an AMA framework, they must all have the same objective of identifying key risks. There are a number of existing tools, such as audit scores and performance indicators that may be acceptable under this definition.

#### IV. Banking Activities and Operational Risk

The above definition of operational risk gives a sense of the breadth of exposure to operational risk that exists in banking today as well as the many interdependencies among risk factors that may result in an operational risk loss. Indeed, operational risk can occur in any activity, function, or unit of the institution.

The definition of operational risk incorporates the risks stemming from people, processes, systems and external events. People risk refers to the risk of management failure, organizational structure or other human resource failures. These risks may be exacerbated by poor training, inadequate controls, poor staffing resources, or other factors. The risk from processes stem from breakdowns in established processes, failure to follow processes, or inadequate process mapping within business lines. System risk covers instances of both disruption and outright system failures in both internal and outsourced operations. Finally, external events can include natural disasters, terrorism, and vandalism.

There are a number of areas where operational risks are emerging. These include:

- Greater use of automated technology has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems;

- Proliferation of new and highly complex products;

- Growth of e-banking transactions and related business applications expose an institution to potential new risks (e.g., internal and external fraud and system security issues);

- Large-scale acquisitions, mergers, and consolidations test the viability of new or newly integrated systems;

- Emergence of institutions acting as large-volume service providers create the need for continual maintenance of high-grade internal controls and back-up systems;

- Development and use of risk mitigation techniques (e.g., collateral, insurance, credit derivatives, netting arrangements and asset securitizations) optimize an institution's exposure to

market risk and credit risk, but potentially create other forms of risk (e.g., legal risk); and

- Greater use of outsourcing arrangements and participation in clearing and settlement systems mitigate some risks while increasing others.

The range of banking activities and areas affected by operational risk must be fully identified and considered in the development of the institution's risk management and measurement plans. Since operational risk is not confined to particular business lines<sup>9</sup>, product types, or organizational units, it should be managed in a consistent and comprehensive manner across the institution. Consequently, risk management mechanisms must encompass the full range of risks, as well as strategies that help to identify, measure, monitor and control those risks.

#### V. Corporate Governance

##### Supervisory Standards

S 1. The institution's operational risk framework must include an independent firm-wide operational risk management function, line of business management oversight, and independent testing and verification functions.

The management structure underlying an AMA operational risk framework may vary between institutions. However, within all AMA institutions, there are three key components that must be evident—the firm-wide operational risk management function, lines of business management, and the testing and verification function. These three elements are functionally independent<sup>10</sup> organizational components, but should work in cooperation to ensure a robust operational risk framework.

##### A. Board and Management Oversight

##### Supervisory Standards

S 2. The board of directors must oversee the development of the firm-wide operational risk framework, as

<sup>9</sup> Throughout this guidance, terms such as "business units" and "business lines" are used interchangeably and refer not only to an institution's revenue-generating businesses, but also to corporate staff functions such as human resources or information technology.

<sup>10</sup> For the purposes of AMA, "functional independence" is defined as the ability to carry out work freely and objectively and render impartial and unbiased judgments. There should be appropriate independence between the firm-wide operational risk management functions, line of business management and staff and the testing/verification functions. Supervisory assessments of independence issues will rely upon existing regulatory guidance (e.g. audit, internal control systems, board of directors/management, etc.)

<sup>8</sup> An institution's definition of risk may encompass other risk elements as long as the supervisory definition is met.