Operational Risk Categories

Operational Risk Area	Description	Information or IT Mapping
Facilities and operating environment risk	Loss or damage to operational capabilities caused by problems with premises, facilities, services or equipment	Business continuity management for IT facilities
Health and safety risk	Threats to the personal health and safety of staff, customers and members of the public	Confidentiality of home addresses, travel schedules, etc.
Information risk	Unauthorized disclosure or modification of information, loss of availability of information, or inappropriate use of information	All aspects of information and IT security
Control frameworks risk	Inadequate design or performance of the existing risk management infrastructure	Business process analysis to identify critical information flows and control points
Legal and regulatory compliance risk	Failure to comply with the laws of the jurisdictions in which business operations are carried out; failure to comply with any regulatory, reporting and taxation standards; failure to comply with contracts; or failure of contracts to protect business interests	Compliance with applicable data protection legislation, cryptographic control regulations, etc.; accuracy, timeliness and quality of information reported to regulators; and content management of all information sent to other parties
Corporate governance risk	Failure of directors to fulfill their personal statutory obligations in managing and controlling the enterprise	Information security policy making, performance measurement and reporting
Reputation risk	The negative effects of public opinion, customer opinion and market reputation, and the damage caused to the brand by failure to manage public relations	Controlling the disclosure of confidential information; presenting a public image of a well-managed enterprise

Operational Risk Area	Description	Information or IT Mapping
Strategic risk	Failure to meet the long-term strategic goals of the business, including dependence on any estimated or planned outcomes that may be in the control of third parties	Managing the quality and granularity of information on which strategic business decisions are based (e.g., mergers, acquisitions, disposals)
Processing and behavioral risk	Problems with service or product delivery caused by failure of internal controls or information systems, lack of employee integrity, errors and mistakes, or through weaknesses in operating procedures	All aspects of information systems security and the security-related behavior of employees in carrying out their tasks
Technology risk	Failure to plan, manage and monitor the performance of technology-related projects, products, services, processes, staff and delivery channels	Failure of information and communications technology systems and the need for business continuity management
Criminal and illicit acts risk	Loss or damage caused by fraud, theft, willful neglect, gross negligence, vandalism, sabotage, extortion, etc.	Provision of security services and mechanisms to prevent all types of cybercrime
Human resources risk	Failure to recruit, develop or retain employees with the appropriate skills and knowledge or to manage employee relations	Need for policies protecting employees from sexual harassment, racial abuse, etc., through corporate email systems, etc.
Supplier risk	Failure to evaluate adequately the capabilities of suppliers leading to breakdowns in the supply process or substandard delivery of supplied goods and services; failure to understand and manage supply chain issues	Outsourced service delivery of IT or other business information processing activities

Operational Risk Area	Description	Information or IT Mapping
Management information risk	Inadequate, inaccurate, incomplete or untimely provision of information to support the management decision- making process	Managing the accuracy, integrity, currency, timeliness and quality of information used for management decision support
Ethics risk	Damage caused by unethical business practices, including those of associated business partners. Issues include racial and religious discrimination, exploitation of child labor, pollution, environmental issues, negative behavior toward disadvantaged groups, etc.	Ethical collection, storage and use of information; management of information content on websites, intranets, and in corporate emails and instant messaging systems
Geopolitical risk	Loss or damage in some countries caused by political instability, poor quality of infrastructure in developing regions, or cultural differences and misunderstandings	Managing all aspects of information security and IT systems' security in regions where the enterprise has business operations but where there is special geopolitical risk
Cultural risk	Failure to deal with cultural issues affecting employees, customers or other stakeholders. These include language, religion, morality, dress codes and other community customs and practices.	Management of information content on websites, intranets, and in corporate emails and instant messaging systems
Climate and weather risk	Loss or damage caused by unusual climate conditions, including drought, heat, flood, cold, storm, winds, etc.	Business continuity management for IT facilities

Source: Copyright SABSA Institute, www.sabsa.org. Reproduced with permission.