



Appendix F1-2

Operational Risk Management Mapping to ICT

Operational Risk Areas	Description	Information or ICT 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 ICT facilities
Health & 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 Security Risk	Unauthorised disclosure or modification to information, or loss of availability of information, or inappropriate use of information	All aspects of information and ICT 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 & Regulatory Compliance Risk	Failure comply with the laws of the countries in which business operations are carried out, or failure to comply with any regulatory, reporting and taxation standards, or failure to comply with contracts, or failure of contracts to protect business interests	Compliance with data protection legislation, cryptographic control regulations, etc. Also accuracy, timeliness and quality of information reported to regulators. Also content management of all information sent to other parties
Corporate Governance Risk	Failure of directors to fulfil their personal statutory obligations in managing and controlling the company	Information security policy making, performance measurement and reporting
Reputation Risk	The negative effects of public opinion, customer opinion, market reputation and the damage caused to the brand by failure to manage public relations	Controlling the disclosure of confidential information. Also presenting a public image of a 'well-managed' enterprise

Operational Risk Areas	Description	Information or ICT 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 (such as mergers, acquisitions, disposals)
Processing and Behavioural Risk	Problems with service or product delivery caused by failure of internal controls, information systems, employee integrity, or by errors and mistakes, or through weaknesses in operating procedures	All aspects of information systems security and the security-related behaviour 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
Project Management Risk	Failure to plan and manage the resources required for achieving tactical project goals, leading to budget overruns or time overruns or both, or leading to failure to complete the project. Also the technical failure of a project or the failure to manage the integration aspects with existing parts of the business and the impact that changes can have on business operations	Management of all information security related projects
Criminal and Illicit Acts Risk	Loss or damage caused by fraud, theft, wilful neglect, gross negligence, vandalism, sabotage, extortion, etc.	Provision of security services and mechanisms to prevent all types of cyber-crime

Operational Risk Areas	Description	Information or ICT Mapping
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 e-mail systems etc
Supplier Risk	Failure to evaluate adequately the capabilities of suppliers leading to breakdowns in the supply process or sub-standard delivery of supplied goods and services. Also failure to understand and manage the supply-chain issues	Out-sourced service delivery of ICT or other business information processing activities
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 labour, pollution, environmental and so-called 'green issues', behaviour to disadvantaged groups, etc.	Ethical collection, storage and use of information. Management of information content on web-sites, Intranets and in corporate e-mails and corporate instant messaging systems
Geo-political Risk	Loss or damage in some countries, caused by political instability, or by poor quality of infrastructure in developing regions, or by cultural differences and misunderstandings	Managing all aspects of information security and ICT systems security in regions where the enterprise has business operations but where there are special geo-political risks.

Operational Risk Areas	Description	Information or ICT Mapping
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 web-sites, Intranets and in corporate e-mails and corporate 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 ICT facilities