Risk Taxonomy

15. Annexures

ANNEXURE 1: OPERATIONAL RISK EVENT MODEL

Level 2	Process failures	Internal fraud	External fraud	Accidents, health and safety and acts of nature	Employment practices and workplace safety	Sales, products and business practice	Compliance and regulatory	System failures
Level 3	Project failure	Commission abuse	Commission abuse	Injury to employees & customers	Recruitment practice	Miss-selling (including advice, disclosure and transparency)	Regulatory breaches	Systems availability
	Product design flaws	Customers take on fraud	Invoice fraud	Accidents and acts of nature: Sensitive data	Harassment	Vendors	Tax	Sensitive data integrity: Systems
	Marketing material	Client instruction fraud	Claims fraud	Accidental damage to property	Unfair dismissal	Customer contractual obligations	Sanctions	Sensitive data confidentiality and security: Systems
	Product pricing	Payment and settlement fraud	Payment and settlement fraud	Deliberate damage to property	Employee relations	Fiduciary duty of care	Money laundering & terrorist financing	Cloud security
	Customers take on data	Unauthorised activity	Client instruction fraud	Environmental hazards – noise, light, cold, dust, heat etc	Safe environment	Conflicts of Interest	Litigation	Hardware failure
	Payment & settlement	Theft	Theft	Psycho-social hazards – fatigue, work related stress, workplace harassment and occupational violence	Diversity and discrimination	Bribery and Corruption	Mishandling of legal processes	Software failure
	Premium/Fee collection	Credit and debit card fraud	Systems security	Ergonomic hazards – incorrect use of workstation/chair, akward posture	Training and skills	Improper business or market practices	Contractual rights/obligation failures	Network failure
	Sensitive data	Ghost employee	Credit and debit card fraud	Safety hazards – Spills on floor, incorrect use of ladders, electrical hazards, confined spaces etc	Reward and recognition	Product flaws	Bribery and corruption	Data loss/Improper access to data
	Suppliers & outsourcing	Unauthorised Masterfile changes	Hacking, phishing and pharming			Customer advice	Ineffective relationship with regulators	Unavailability of data

Level 2	Process failures	Internal fraud	External fraud	Accidents, health and safety and acts of nature	Employment practices and workplace safety	Sales, products and business practice	Compliance and regulatory	System failures
	Capital and funding	Financial statement manipulation	Third-party/vendor fraud			Post-sale barriers	dequate response to regulatory change	Poor data quality
	Model errors	Skimming	Agent/broker/intermediary fraud			Insider trading	Improper licensing/certification/registration	Inadequate data architecture
	Contractual agreements	Tax fraud				Customer mistreatment/Failure to fulfil duties to customers	Prudential risk	Inadequate data storage/retention and destruction management
	Reinsurance					Improper/Unethical marketing	External financial and regulatory reporting failure	
	Communication					Improper product design		
	Capital allocation					Breach of code of conduct and misbehavior		
	Compliants							
	Valuations							
	People/Productivity							
	Budget overrun							
	Financial Misstatement							
	Transaction capture, execution, and maintenance							
	Third-party management control failure							
	Model/methodology design failure							
	Model implementation/application error							

ANNEXURE 2: OPERATIONAL CAUSE MODEL

Level 1	People	System	Process	External
Level 2	Inadequate internal environment (Organisational Culture)	Unreliability	Inadequate design, formalization and update of processes and procedures	Business Environment Changes
	Intentional unauthorised/malicious activity (Intentional)	Capacity constraints	Inefficient method of processes execution	Criminal Activities (External)
	Human error/ negligence (unintentional)	Stability	Inadequate process monitoring and controls	Accidents (3rd Parties)
	Inadequate compensation system	Inadequacy of security systems and information storage	Inadequate communication and reporting	Natural disasters
	Inadequate human resources selection	Usability and functionality	Inadequate contracts and outsourcing activities monitoring	Political Environment
	Inadequate development of human resources	Scalability	Non-existent	Regulatory Environment
	Inadequate staffing and back up mechanisms	Misaligned infrastructure/ architecture	Change/project mismanagement	Contractual breach
	Inadequate administrative human resources management	Inadequacy of hardware and software	Governance failure	Physical infrastructure
	Other human resources inadequacies	Lack of maintenance/unsupported legacy		Micro- and/or macro-economic environment
	Ineffective roles and responsibilities	Inadequate testing/development		Terrorism/external attacks
	Miscommunication	Release/deployment issues		Geopolitical/Socio-ecomical
		Misconfiguration		
		Exploitation of IT security vulnerability		
		Technology related planning issues		

ANNEXURE 3: SASRIA RISK TAXONOMY

Level 1 and Level 2 risk taxonomy:

Level 1	Strategic	Insurance	Market	Credit & Default	Operational
Level 2	Expenses	Premium	Interest rates	Concentration	Process failures
	New business (volume)	CAT	Equity	Default	Internal fraud
	Lapse/renewals	Reserve	Property	Sovereign	External fraud
	Investment performance	Claims	Currency		Accidents and acts of nature
	Distribution channels		Liquidity		Employment practices
	Product choices				Sales, products & business practice
	IT Investments				Compliance and regulatory
	Governance				System failures
	People				
	Key man/Key team				
	Objectives				
	Stakeholder Management				