Postgraduate Certificate in Risk Management for Central Banks (Bangladesh)

Operational Risk Management

Adverse Event – an incident that results in loss, damage, or a breach of policy. Related: incident, loss event. Example: a system outage that prevents transaction processing. Practical application: logging and root-cause analysis. Challenge: distinguishing minor glitches from systemic risks.

Aggregation – the process of combining individual risk exposures to assess total risk. Related: correlation, concentration risk. Example: summing fraud losses across branches. Practical application: stress-testing aggregated operational risk. Challenge: modeling dependencies accurately.

Alert Fatigue – desensitisation of staff to frequent warnings, leading to missed critical alerts. Related: monitoring, alarm overload. Example: daily system alerts ignored by IT team. Practical application: tiered alert thresholds. Challenge: balancing sensitivity with relevance.

Asset-Based Approach – assessing risk by evaluating the assets (people, processes, technology) that support operations. Related: risk inventory, asset mapping. Example: reviewing the reliability of the payment gateway server. Practical application: prioritising controls on high-value assets. Challenge: keeping asset registers current.

Audit Trail – a chronological record of activities that provides evidence of actions taken. Related: log, forensic evidence. Example: transaction logs showing user access times. Practical application: supporting investigations and compliance checks. Challenge: ensuring integrity and accessibility of logs.

Automation Risk – risk arising from reliance on automated processes and systems. Related: technology risk, system failure. Example: automated fund transfer error due to coding bug. Practical application: periodic code reviews and test environments. Challenge: detecting hidden logic errors.

Baseline Controls – the minimum set of controls required to mitigate identified risks. Related: control framework, minimum standards. Example: dual-authorization for large payments. Practical application: embedding controls in SOPs. Challenge: avoiding “checkbox” compliance without effectiveness.

Business Continuity Planning (BCP) – strategies to ensure critical functions continue during disruptions. Related: disaster recovery, resilience. Example: alternate data centre activation after a flood. Practical application: regular BCP drills. Challenge: maintaining up-to-date recovery sites.

Business Impact Analysis (BIA) – assessment of the effects of disruption on key activities. Related: risk assessment, criticality. Example: measuring loss of revenue if the clearing system is down for 24 hours. Practical application: prioritising recovery objectives. Challenge: quantifying intangible impacts.

Capacity Risk – risk that operational capacity is insufficient to meet demand. Related: resource risk, overload. Example: insufficient staff during peak transaction periods causing delays. Practical application: dynamic staffing models. Challenge: forecasting demand spikes accurately.

Case Study – a detailed examination of a real-world incident to derive lessons. Related: learning, best practice. Example: analysis of a cyber-attack on a regional bank. Practical application: training modules for staff. Challenge: ensuring relevance to the local context.

Change Management – systematic approach to handling modifications in processes or systems. Related: governance, transition. Example: rollout of a new core banking platform. Practical application: impact assessments and stakeholder communication. Challenge: resistance from employees accustomed to legacy systems.

Chaos Engineering – intentional injection of failures to test system resilience. Related: fault injection, robustness testing. Example: disabling a network node to observe failover behavior. Practical application: improving incident response. Challenge: controlling the scope to avoid unintended service disruption.

Clearance of Exceptions – formal approval to deviate from standard controls for a limited period. Related: waiver, risk acceptance. Example: allowing a temporary reduction in segregation of duties during system migration. Practical application: documented exception logs. Challenge: monitoring and timely revocation of exceptions.

Co-Location Risk – vulnerability arising from physical proximity of critical assets. Related: geographic concentration, clustering. Example: multiple data centres located in the same flood-prone district. Practical application: diversifying locations. Challenge: balancing cost with risk reduction.

Compliance Risk – risk of legal or regulatory sanctions due to non-adherence. Related: regulatory risk, enforcement. Example: failure to report large cash transactions as required by AML laws. Practical application: compliance monitoring dashboards. Challenge: rapidly evolving regulatory environment.

Control Gap – deficiency where existing controls do not fully address a risk. Related: control weakness, remediation. Example: lack of two-factor authentication for remote access. Practical application: gap analysis and remediation planning. Challenge: prioritising limited resources.

Control Self-Assessment (CSA) – process where owners evaluate the effectiveness of their own controls. Related: self-audit, internal review. Example: branch managers rating their fraud detection controls. Practical application: fostering ownership of risk. Challenge: ensuring objectivity and avoiding bias.

Counterparty Risk – risk that a party to a transaction fails to meet obligations. Related: credit risk, settlement risk. Example: a correspondent bank unable to process payments due to operational failure. Practical application: due-diligence and exposure limits. Challenge: hidden operational weaknesses of counterparties.

Critical Incident – a severe event that disrupts essential services. Related: major outage, emergency. Example: ransomware encrypting the central bank's payment system. Practical application: incident command structure activation. Challenge: rapid escalation and communication.

Cyber-Risk – risk of loss or damage from electronic attacks or failures. Related: information security, IT risk. Example: phishing attack compromising employee credentials. Practical application: regular penetration testing. Challenge: staying ahead of sophisticated threat actors.

Data Integrity – assurance that data is accurate, complete, and unaltered. Related: data quality, validation. Example: corrupted transaction records due to software bug. Practical application: checksum verification routines. Challenge: detecting subtle data anomalies.

Data Loss Prevention (DLP) – technologies and policies to prevent unauthorized data exfiltration. Related: security, leakage. Example: blocking outbound emails containing sensitive customer data. Practical application: DLP rules integrated with email gateway. Challenge: balancing security with business workflow.

De-Risking – systematic reduction of risk exposure. Related: mitigation, risk reduction. Example: outsourcing non-core processes to specialised vendors. Practical application: risk-based vendor selection. Challenge: transferring risk without creating new dependencies.

Dependency Mapping – visualisation of inter-relationships among processes, systems, and suppliers. Related: network analysis, critical path. Example: mapping how payment clearing depends on third-party messaging services. Practical application: identifying single points of failure. Challenge: keeping the map current amid frequent changes.

Disaster Recovery (DR) – set of measures to restore IT systems after a catastrophic event. Related: BCP, restoration. Example: restoring backup servers after a fire. Practical application: recovery time objectives (RTO) and recovery point objectives (RPO). Challenge: testing DR without disrupting production.

Duplicate Transaction Risk – risk of processing the same transaction more than once. Related: reconciliation, duplication. Example: double posting of a wire transfer due to interface error. Practical application: uniqueness checks in transaction processing. Challenge: detecting duplicates in high-volume environments.

Economic Capital – amount of capital a bank holds to absorb losses from operational risk. Related: risk appetite, capital adequacy. Example: allocating BDT 500 million to cover potential fraud losses. Practical application: internal capital allocation models. Challenge: measuring operational risk with sufficient precision.

Emerging Risk – new or evolving risk that may become significant. Related: horizon scanning, trend analysis. Example: adoption of blockchain technologies introducing novel operational challenges. Practical application: periodic risk horizon workshops. Challenge: limited historical data for quantification.

Enterprise Risk Management (ERM) – holistic approach to identifying, assessing, and managing all risk categories. Related: risk framework, governance. Example: integrating operational risk metrics into the central bank's risk dashboard. Practical application: board-level risk reporting. Challenge: aligning diverse risk silos.

Escalation Protocol – predefined steps for raising awareness of a serious incident. Related: incident management, communication. Example: notifying senior management within 30 minutes of a system breach. Practical application: clear escalation matrix. Challenge: ensuring timely response across time zones.

Event Management – systematic handling of incidents from detection to resolution. Related: incident lifecycle, ticketing. Example: using an ITSM tool to track a payment processing error. Practical application:

root-cause analysis reports. Challenge: avoiding siloed event handling.

External Audit – independent examination of an organisation's controls by an outside party. Related: assurance, compliance. Example: audit of the central bank's outsourcing arrangements. Practical application: audit findings incorporated into remediation plans. Challenge: coordinating audit schedules with operational demands.

Failure Mode – specific way in which a component or process can fail. Related: FMEA, fault analysis. Example: server overheating leading to shutdown. Practical application: failure mode identification during risk workshops. Challenge: capturing rare but high-impact modes.

Fault Tree Analysis (FTA) – diagrammatic method to explore cause-and-effect relationships leading to a top-level event. Related: event tree, root cause. Example: constructing a fault tree for a payment system outage. Practical application: prioritising corrective actions. Challenge: complexity grows with system size.

Financial Crime Risk – risk of losses due to fraud, money laundering, or terrorist financing. Related: AML, sanctions compliance. Example: insider collusion to divert funds. Practical application: transaction monitoring systems. Challenge: staying ahead of sophisticated schemes.

First-Line of Defense – operational units that own and manage risks directly. Related: risk ownership, business units. Example: treasury department managing its own operational risk registers. Practical application: embedding risk awareness in daily activities. Challenge: balancing performance pressures with risk controls.

Flood Risk – vulnerability to water-related damage affecting facilities or infrastructure. Related: natural hazard, geographic risk. Example: a river overflow inundating a data centre. Practical application: flood-proofing critical equipment. Challenge: predicting rare extreme events.

Framework Alignment – ensuring that operational risk practices conform to a recognised standard. Related: Basel III, ISO 31000. Example: mapping internal policies to the Basel Operational Risk Framework. Practical application: gap-assessment exercises. Challenge: reconciling local regulations with global standards.

Fraud Risk – risk of intentional deception resulting in financial loss. Related: internal fraud, external fraud. Example: a teller manipulating account balances. Practical application: segregation of duties and surprise audits. Challenge: detecting collusion among multiple parties.

Functional Risk – risk arising from the execution of a specific business function. Related: process risk, line risk. Example: risk of errors in foreign exchange settlement. Practical application: function-specific risk registers. Challenge: ensuring consistent risk definitions across functions.

Governance Structure – organisational arrangement for overseeing risk management. Related: board, risk committee. Example: establishing an Operational Risk Committee reporting to the Governor. Practical application: clear charter and reporting lines. Challenge: avoiding overlapping responsibilities.

Heat Map – visual representation of risk levels using colour coding. Related: risk matrix, dashboard. Example: plotting likelihood versus impact for operational incidents. Practical application: prioritising risk

mitigation efforts. Challenge: subjectivity in assigning scores.

Incident Response Plan (IRP) – detailed actions to be taken when a security incident occurs. Related: cyber-incident, playbook. Example: steps for isolating infected workstations after a malware detection. Practical application: regular IRP drills. Challenge: maintaining plan relevance amid technology changes.

Indemnity – contractual provision to compensate for losses incurred. Related: insurance, liability. Example: vendor agreement includes indemnity for data breach caused by the vendor. Practical application: negotiating indemnity clauses. Challenge: enforceability across jurisdictions.

Information Security Management System (ISMS) – set of policies and procedures to protect information assets. Related: ISO 27001, confidentiality. Example: implementing access controls for the central bank's statistical database. Practical application: periodic ISMS audits. Challenge: integrating ISMS with broader operational risk framework.

Infrastructure Risk – risk associated with physical and technological foundations of operations. Related: asset risk, system reliability. Example: aging power supply causing frequent outages. Practical application: infrastructure renewal programmes. Challenge: budget constraints and long lead times.

Internal Audit – independent, objective assurance function within the organisation. Related: control testing, risk assessment. Example: audit of the cash handling process at branch offices. Practical application: audit recommendations feeding into risk registers. Challenge: maintaining auditor independence.

Key Risk Indicator (KRI) – metric used to signal rising risk exposure. Related: metric, early warning. Example: number of failed login attempts exceeding a threshold. Practical application: KRI dashboards for senior management. Challenge: selecting indicators that truly predict incidents.

Liquidity Risk (Operational) – risk of being unable to meet short-term cash needs due to operational failures. Related: funding risk, cash flow. Example: payment system downtime preventing settlement of interbank transfers. Practical application: contingency cash buffers. Challenge: quantifying operational impact on liquidity.

Loss Event – occurrence that leads to a measurable loss. related: incident, claim. Example: a system glitch causing a BDT 2 million overpayment. Practical application: recording loss events in the operational risk database. Challenge: consistent classification of loss types.

Loss Distribution Approach (LDA) – statistical method to model frequency and severity of loss events. related: modeling, VaR. Example: using LDA to estimate annual operational loss capital. Practical application: Monte-Carlo simulations. Challenge: limited data for rare, high-impact events.

Loss Event Type (LET) – categorisation of loss events by cause. related: taxonomy, classification. Example: "External fraud" as a LET. Practical application: standardising reporting across departments. Challenge: ensuring consistent tagging by reporters.

Loss Event Severity – magnitude of loss resulting from an event. related: impact, monetary loss. Example: BDT 10 million loss due to a cyber-theft. Practical application: severity thresholds for escalation. Challenge:

capturing indirect or reputational losses.

Loss Event Frequency – number of occurrences of a specific loss type within a period. related: count, occurrence rate. Example: three instances of payment processing errors in a quarter. Practical application: trend analysis to detect rising frequencies. Challenge: small sample sizes hindering statistical confidence.

Loss Event Reporting – systematic capture and communication of loss information. related: incident log, reporting line. Example: mandatory reporting of any loss exceeding BDT 500 000. Practical application: automated reporting workflows. Challenge: under-reporting due to fear of repercussions.

Macro-Economic Shock – large-scale economic event that can amplify operational risk. related: systemic risk, external shock. Example: sudden currency devaluation stressing payment processing capacities. Practical application: scenario analysis incorporating macro variables. Challenge: linking macro indicators to operational outcomes.

Management Information System (MIS) – platform for collecting and presenting risk data. related: reporting, analytics. Example: dashboard displaying real-time KRI values. Practical application: enabling data-driven decision-making. Challenge: ensuring data quality and timeliness.

Management Oversight – supervisory role of senior leaders in risk governance. related: board, risk committee. Example: Governor reviewing monthly operational risk heat maps. Practical application: regular risk review meetings. Challenge: avoiding “risk-blindness” due to operational pressures.

Market Risk (Operational) – risk that market-related processes fail, affecting operations. related: trading systems, settlement. Example: failure of market data feed causing valuation errors. Practical application: redundant data feeds. Challenge: synchronising multiple market sources.

Mitigation Plan – set of actions designed to reduce risk likelihood or impact. related: remediation, control improvement. Example: implementing multi-factor authentication to mitigate credential theft. Practical application: assigning owners and deadlines. Challenge: tracking progress across many initiatives.

Monitoring – ongoing observation of risk indicators and control effectiveness. related: surveillance, oversight. Example: daily review of failed batch jobs. Practical application: automated alerts for threshold breaches. Challenge: alarm fatigue and false positives.

Near-Miss – an event that could have resulted in loss but did not. related: close call, warning. Example: a transaction flagged but corrected before execution. Practical application: reporting near-misses to identify systemic weaknesses. Challenge: encouraging staff to report without fear.

Network Risk – risk arising from interconnections among internal and external systems. related: dependency, cyber-risk. Example: a third-party API failure cascading to the central bank’s reporting system. Practical application: network segmentation and redundancy. Challenge: mapping complex, multi-vendor networks.

Operational Risk Appetite – the level of operational risk a bank is willing to accept. related: tolerance, threshold. Example: tolerating minor processing delays up to 0.5 % of total transactions. Practical

application: setting quantitative limits for KRIs. Challenge: aligning appetite with strategic objectives.

Operational Risk Framework – structured set of policies, processes and tools for managing operational risk. related: Basel III, ERM. Example: adopting the Basel Operational Risk Framework tailored for Bangladesh. Practical application: comprehensive risk registers and reporting lines. Challenge: ensuring full implementation across all units.

Operational Risk Indicator (ORI) – metric that reflects the performance of operational risk controls. related: KRI, metric. Example: percentage of incidents resolved within SLA. Practical application: benchmarking against industry standards. Challenge: selecting indicators that drive meaningful behaviour change.

Operational Resilience – ability to continue critical functions during disruptions. related: BCP, recovery. Example: maintaining payment clearing services during a cyber-attack. Practical application: resilience testing and scenario planning. Challenge: measuring resilience in quantitative terms.

Outsourcing Risk – risk transferred to a third-party provider. related: vendor risk, service level. Example: reliance on an external data-processing firm for statistical releases. Practical application: due-diligence and ongoing performance monitoring. Challenge: loss of direct control and visibility.

Over-Reliance Risk – excessive dependence on a single process, technology or supplier. related: concentration, single point of failure. Example: a single core banking system handling all transactions. Practical application: diversification and backup solutions. Challenge: cost of redundancy versus perceived risk.

Penetration Testing – simulated cyber-attack to evaluate security controls. related: ethical hacking, vulnerability assessment. Example: external firm attempts to breach the central bank's network. Practical application: remediation of identified weaknesses. Challenge: ensuring test scope covers critical assets.

Performance Risk – risk that operational performance falls below expectations. related: service level, KPI. Example: processing times exceeding defined thresholds during peak periods. Practical application: performance dashboards and corrective action plans. Challenge: balancing speed with accuracy.

Policy Violation – breach of established rules or procedures. related: non-compliance, misconduct. Example: employee bypassing segregation of duties for convenience. Practical application: disciplinary procedures and retraining. Challenge: detecting hidden violations.

Process Mapping – visual representation of workflow steps and decision points. related: flowchart, documentation. Example: mapping the end-to-end payment settlement process. Practical application: identifying bottlenecks and control points. Challenge: keeping maps current as processes evolve.

Process Risk – risk arising from inadequacies in business processes. related: procedural risk, workflow. Example: manual reconciliation errors due to insufficient checks. Practical application: automating repetitive tasks. Challenge: change management for new processes.

Probability of Failure on Demand (PFD) – likelihood that a safety function will not perform when required. related: reliability, safety integrity. Example: PFD of 0.02 for an automated fraud detection system. Practical

application: risk-based testing frequency. Challenge: estimating PFD for complex systems.

Qualitative Risk Assessment – evaluation based on descriptive criteria rather than numerical data. related: scoring, expert judgment. Example: rating risk likelihood as “high” and impact as “moderate”. Practical application: initial screening of emerging risks. Challenge: subjectivity and lack of comparability.

Quantitative Risk Assessment – evaluation using numerical data and statistical techniques. related: modelling, loss distribution. Example: estimating a 99.9 % VaR for operational losses. Practical application: capital allocation calculations. Challenge: data scarcity for rare events.

Rapid Response Team (RRT) – specialised group tasked with immediate incident handling. related: incident response, crisis management. Example: IT security experts mobilised after a ransomware alert. Practical application: predefined RRT activation criteria. Challenge: maintaining skill readiness.

Reputational Risk (Operational) – risk of damage to public image due to operational failures. related: brand, stakeholder trust. Example: media coverage of a payment system outage. Practical application: communication protocols and media training. Challenge: quantifying reputational impact.

Risk Appetite Statement – formal declaration of the amount of risk the institution is prepared to accept. related: tolerance, policy. Example: “The central bank tolerates operational loss events up to BDT 1 million per annum.” Practical application: guiding risk-taking decisions. Challenge: translating narrative into measurable limits.

Risk Assessment – systematic identification and evaluation of risks. related: analysis, appraisal. Example: assessing the likelihood of a cyber-attack on the foreign exchange platform. Practical application: risk registers and prioritisation matrices. Challenge: ensuring comprehensive coverage.

Risk Culture – shared values and behaviours regarding risk awareness and management. related: tone from the top, attitudes. Example: encouraging staff to report errors without fear of punishment. Practical application: risk-aware training programmes. Challenge: changing entrenched behaviours.

Risk Control Matrix (RCM) – tool linking risks to controls and testing procedures. related: mapping, audit. Example: linking “fraud risk” to “dual-approval” control and testing its effectiveness. Practical application: facilitating internal audit planning. Challenge: maintaining accuracy as controls evolve.

Risk Event – any occurrence that could affect the achievement of objectives. related: incident, trigger. Example: a power failure affecting data centre operations. Practical application: event classification and response planning. Challenge: differentiating risk events from routine variations.

Risk Register – central repository of identified risks, their assessments and mitigation actions. related: database, tracking. Example: a spreadsheet listing all operational risk categories with owners. Practical application: regular updates and board reporting. Challenge: data consistency and owner accountability.

Risk Tolerance – acceptable deviation from risk appetite for a specific risk type. related: limits, thresholds. Example: allowing a 10 % increase in processing errors during system upgrades. Practical application: tolerance bands for KRIs. Challenge: setting tolerances that are neither too tight nor too lax.

Risk Transfer – shifting risk to another party, usually via insurance or contracts. related: indemnity, outsourcing. Example: purchasing cyber-insurance to cover breach costs. Practical application: evaluating policy coverage against risk profile. Challenge: high premiums and coverage exclusions.

Risk-Based Supervision (RBS) – regulatory approach focusing on areas with higher risk exposure. related: supervisory framework, Basel III. Example: the Bangladesh central bank prioritising supervision of payment system operators with high operational risk scores. Practical application: targeted inspections. Challenge: obtaining reliable risk data from institutions.

Scenario Analysis – technique that explores the impact of hypothetical events. related: stress testing, what-if. Example: modelling the effect of a nationwide cyber-attack on payment clearing. Practical application: informing contingency planning. Challenge: selecting plausible yet severe scenarios.

Service Level Agreement (SLA) – contractual commitment specifying performance standards. related: metric, vendor contract. Example: SLA requiring 99.9 % system uptime for a third-party data provider. Practical application: monitoring compliance and penalties. Challenge: negotiating realistic service levels.

Single Point of Failure (SPOF) – component whose failure would cause a system-wide outage. related: dependency, redundancy. Example: a single database server handling all transaction records. Practical application: introducing redundant servers. Challenge: identifying hidden SPOFs in complex architectures.

Social Engineering – manipulation technique to trick individuals into revealing confidential information. related: phishing, insider threat. Example: a caller impersonating a senior manager to obtain login credentials. Practical application: awareness training and verification procedures. Challenge: evolving tactics that bypass technical controls.

Software Bug – defect in code causing unintended behaviour. related: defect, error. Example: a rounding error leading to miscalculated interest. Practical application: rigorous testing and code reviews. Challenge: detecting bugs in legacy systems with limited documentation.

Stakeholder Communication – exchange of information with parties interested in risk outcomes. related: reporting, transparency. Example: informing commercial banks about upcoming changes to the payment system. Practical application: regular newsletters and briefings. Challenge: balancing confidentiality with openness.

Strategic Risk (Operational) – risk that strategic decisions lead to operational failures. related: business risk, misalignment. Example: launching a new digital platform without adequate operational support. Practical application: strategic risk assessments before major initiatives. Challenge: forecasting operational implications of strategic moves.

Stress Testing – analysis of how extreme conditions affect risk exposures. related: scenario analysis, resilience. Example: testing operational loss capital under a severe cyber-attack scenario. Practical application: regulatory reporting and internal capital adequacy. Challenge: modelling low-probability, high-impact events.

Supply Chain Risk – risk arising from disruptions in the flow of goods or services. related: vendor risk, logistics. Example: a key hardware supplier experiencing a strike, delaying server upgrades. Practical application: multi-sourcing and inventory buffers. Challenge: visibility into upstream suppliers' risk controls.

Syndicated Loan Processing Risk – operational risk specific to handling multi-lender loan agreements. related: credit risk, coordination. Example: misallocation of loan proceeds due to inconsistent data feeds. Practical application: standardised data exchange protocols. Challenge: coordinating across multiple institutions.

Systemic Operational Risk – risk that a failure in one institution could cascade throughout the financial system. related: contagion, network risk. Example: a major payment system outage affecting all banks. Practical application: joint contingency planning among central banks. Challenge: aligning incentives for collective risk mitigation.

Technology Risk – risk associated with the use, failure, or obsolescence of technology. related: IT risk, cyber-risk. Example: unsupported operating system leading to security vulnerabilities. Practical application: technology lifecycle management. Challenge: rapid innovation outpacing governance processes.

Third-Party Risk – risk arising from reliance on external service providers. related: outsourcing, vendor management. Example: a cloud provider suffering a data centre outage. Practical application: third-party risk assessments and contractual clauses. Challenge: limited visibility into provider's internal controls.

Threat Intelligence – information about potential or active threats that could impact operations. related: cyber-risk, awareness. Example: receiving alerts about a new ransomware variant targeting banks. Practical application: integrating intelligence feeds into security operations. Challenge: filtering noise and ensuring relevance.

Transaction Monitoring – systematic review of financial transactions to detect suspicious activity. related: AML, fraud detection. Example: flagging unusually large cross-border transfers. Practical application: rule-based and machine-learning models. Challenge: balancing detection rates with false positives.

Turnover Risk – risk associated with high staff turnover affecting continuity. related: human resources, knowledge loss. Example: loss of key IT staff leading to gaps in system maintenance. Practical application: succession planning and knowledge transfer. Challenge: retaining specialised talent in a competitive market.

Undertaking Risk – risk that a new product or service fails to meet operational expectations. related: project risk, launch risk. Example: rollout of a mobile banking app experiencing performance bottlenecks. Practical application: phased pilots and user testing. Challenge: scaling from pilot to full deployment.

Unforeseen Event – incident that was not anticipated in risk assessments. related: black swan, surprise. Example: a sudden earthquake disrupting a data centre. Practical application: flexible response plans and reserve resources. Challenge: limited predictive capability.

Value-At-Risk (VaR) – Operational – statistical measure of potential loss over a defined period at a given confidence level. related: LDA, capital. Example: 99 % VaR of BDT 5 million for operational losses. Practical

application: setting capital buffers. Challenge: model risk and data limitations.

Vendor Management – process of overseeing third-party relationships to ensure performance and risk mitigation. related: outsourcing, SLA. Example: quarterly reviews of a data-analytics provider. Practical application: vendor scorecards and corrective action plans. Challenge: aligning vendor incentives with risk appetite.

Verification Process – systematic check to confirm accuracy and completeness of data or actions. related: validation, audit. Example: double-checking settlement amounts before final posting. Practical application: automated reconciliation tools. Challenge: avoiding over-reliance on manual checks.

Virtualisation Risk – risk linked to the use of virtual machines and cloud environments. related: technology risk, shared infrastructure. Example: hypervisor vulnerability enabling cross-VM attacks. Practical application: segmentation and regular patching. Challenge: managing security across dynamic workloads.

Waterfall Model Risk – risk inherent in sequential development approaches that limit flexibility. related: project risk, methodology. Example: late discovery of requirements causing costly rework. Practical application: adopting agile practices for operational projects. Challenge: cultural shift and training needs.

Workforce Resilience – capacity of staff to adapt to operational stresses and disruptions. related: human capital, training. Example: staff effectively handling surge in transaction volume during a holiday season. Practical application: cross-training and flexible rostering. Challenge: preventing burnout and maintaining morale.

Zero-Day Vulnerability – previously unknown security flaw that can be exploited before a patch is released. related: cyber-risk, patch management. Example: a newly discovered exploit targeting the central bank's web portal. Practical application: rapid incident response and isolation. Challenge: limited time to develop mitigations.