Policy Code: RM-4 Operational Risk

Purpose:

The following policy has been developed to support the company in identifying, assessing, measuring, and monitoring Operational Risk. This policy also sets out other Operational Risk considerations such as legal, outsourcing, and business continuity risks.

Scope:

The scope of implementing this policy is within the jurisdiction of RM and Department Heads under the direct supervision of the AC and the BOD.

Contents:

1. Governance

BOD

The BOD is responsible for approving and monitoring the Operational RMF.

AC

The AC is responsible for ensuring that Operational Risk management is implemented effectively through sufficient and appropriate policies, procedures, controls, and reports to control the risk. The responsibilities of the AC regarding the oversight of Operational Risk management include:

1) Setting the strategy for the development and implementation of Operational Risk management;

2) Monitoring of ORSAs with high residual risks, and tracking of the implementation of associated action plans;

3) Identification, monitoring, and control of Key Risk Indicators (hereinafter 'KRI'), including review of KRIs that are consistently exceeding threshold limits, or of KRIs that show unusual activity;

4) Establishing objective risk tolerances (quantitative metrics) for Operational Risk, initially for operational loss event reporting, and for other measures as the sophistication of the Operational Risk management process improves;

5) Review of operational loss incidents, both actual and near-misses;

6) Providing advice and approval for amendments to the Operational Risk policy and related guidelines and procedures;

7) Identification, assessment, monitoring, and control of key Operational Risk areas.

2. Risk Management function

The key responsibilities of RM, as carried out by the resource responsible for Operational Risk are as follows:

a.) Understand, implement, and ensure compliance with regulatory requirements, and industry-leading practice standards relating to Operational Risk management;

b.) Effect of changes to the Operational Risk policy in alignment with changes in the company's business;
c.) Formulate and update detailed Operational Risk procedures and ensure that the procedures are implemented throughout the company;
d.) Provide a point of reference and facilitator for the company's staff about the implementation of all Operational Risk related matters within the company, particularly the Own Risk Self-Assessment (ORSA) process, identification of Key Risk Indicators (KRIs), incident reporting, and maintenance of the Operational Loss Database;
e.) Implement, facilitate, monitor, and report on the Operational Risk management processes of identification and assessment, and control and mitigation across the company;
f.) Monitor material Operational Risk losses and highlight these to the AC on a timely basis;
g.) Assist SM in establishing objective risk tolerances (quantitative metrics) for Operational Risk, as the sophistication of the Operational Risk management process improves; and
h.) Establish the process for the company to move towards more advanced measurement approaches for Operational Risk.

3. Departmental Heads (DH)

Departmental Heads are responsible for ensuring that the following are completed:
i) Implementing the Operational Risk policies, processes, and other structures developed within the department/ unit;
ii) Identifying Operational Risks and assessing risks in terms of likelihood and impact;
iii) Identifying and assessing the existing controls and management techniques in terms of their ability to manage the identified risk;
iv) Monitoring the effectiveness of the controls on an ongoing basis;
v) Maintaining adequate documentation of risks, controls, and management techniques;
vi) Periodically and formally reporting to RM on the effectiveness of its management of Operational Risk in the form of Risk and Own Risk Self Assessments (ORSA); and
vii) Promptly reporting on any Operational Risk incidents.

4. Internal Audit (IA)

The Internal Audit Department is responsible for the following Operational Risks:
1) Ensuring adherence to Operational Risk management policies and procedures;

2) Monitoring the implementation and execution of Operational Risk strategies from an independent viewpoint, and advising the BOD AC accordingly;

3) Independently and pragmatically advising management on the necessary regular review processes within the Operational Risk environment, and how and where implementation and ongoing Operational Risk management can be improved; and

4) Independently validating the integrity and administration of Operational Risk models for use within regulatory or internal capital ratio or capital allocation policies.

5. Operational Risk Overview

Operational risk is the risk of financial loss resulting from inadequate or failed internal processes, people, and systems or from external events.

Operational Risk consists of the following risk event categories:

a.) Process Risk

The process of undertaking any transactions entails a chain that includes, transaction risk, documentation/contract risk, and control risk.

b.) People Risk

The differing backgrounds, education, skills, personal expectations/ ambitions, and ethical standards are unique to each individual. Lack of understanding, skill gaps, and above all inadequate training may lead to people risk.

c.) Systems Risk

Takaful companies use various systems to support their operations. Failure or inadequate functioning of systems can result in risks related to ineffective operations, inadequate decision-making, control weaknesses...etc.

d.) Event Risk

Certain uncontrollable events may lead to Operational Risk such as natural disasters or terrorist attacks. Examples of Operational Risks in each category are detailed below:

Table 1. Various Operational Risks with Examples of Risks

Risk source	**Example of risk**
Processes	External data – clients
	External data-Industry
	Internal management information and decisions
	Methodology, modeling, and interpretation
	Contract and documentation risk
	Client service and interaction risk
	Project management
	Financial and strategic management risk
	Financial reporting
People	Key person risk
	Skills/training/people adequacy risk
	Internal fraud and collusion risk
	Culture risk
Systems	Interface risk
	Network risk
	Software risk
	Security risk
	Hardware risk

External events	Legislative and regulatory risk
	Third-party liability
	External fraud risk
	Ethical and environmental risk
	Physical asset risk
	External outsourcing

Operational Risk Management is a key element of a takaful company's ongoing risk management program. The objective of Operational Risk Management is to ensure that Operational Risk is managed and coordinated effectively on a day-to-day basis. It is essential that SM is committed to risk management and that there are rewards and sanctions.

Management will work closely with staff to understand the aims and organization of the business and to get agreement on all aspects of risk management and control.

SM is responsible for the strategic direction of all the operation functions, for determining, implementing, and maintaining standard operation models, and for developing and implementing risk control and compliance standards. In controlling Operational Risk, the company shall only approve new products, transactions, and markets where it possesses the expertise and ability to facilitate effective and proactive risk management (i.e., the ability to identify, capture, measure, control, and report all inherent and related risks).

The company shall maintain levels of resources and systems consistent with current and projected business activity.

The company shall ensure that all business-critical systems are covered by full business continuity procedures and have access to disaster recovery facilities/ plans.

Clear segregation of duties will be established by the company to ensure objectivity, and security and avoid conflicts of interests.

The company will continually evaluate and improve its policies and procedures to effectively support operations and undertake Operational Risk Management across each business line. The company's company has adopted a strict approach to regulatory risk.

The company has zero tolerance for regulatory infringements of any sort.

SM will as far as possible seek to transfer risk which falls outside its appetite either through Re-Takaful, or via judicious use of exclusion and limitation clauses.

The Operational Risk monitoring systems must ensure that both controls and information gathering and reporting systems are effective.

2. Operational Risk Management Strategy

The strategy of the company is to minimize Operational Risk losses. Its Operational Risk strategy comprises risk identification, assessment, measurement management, and reporting.

The establishment and management process is undertaken by RM. The strategy also provides clear guidance on risk appetite or tolerance and policies and procedures for the day-to-day management of Operational Risk. The BOD approves the level of risk appetite and accordingly empowers Management to exercise a cascade of delegated authorities down through the organization to the risk-taking authorities to departments/ units.

The Operational Risk strategy will set the mechanism for establishing risk appetite/ tolerance policies and processes for day-to-day risk management.

3. Internal Controls

A system of internal control is important to ensure the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations.

The company has documented and approved operational policies and procedures that cover major functions such as ICT, financial control, underwriting operations, investment operations, claims handling, and Re-Takaful.

The internal control environment is the framework under which internal controls are developed, implemented, and monitored. No internal control structure can completely prevent errors, illegal acts, or fraudulent activities. Nevertheless, the

company will periodically carry out assessments of the key areas of its operations that are susceptible to these risks and ensure that sufficient and effective control mechanisms are in place to safeguard the assets of the company.

3.1 Internal Control Techniques

Separating functions is the most basic tool for designing internal control systems. It establishes levels and lines of authority, the appropriate delegation of duties, and fixed responsibilities. Transactions may be reviewed before or after they have occurred. Prior review helps prevent improper and unauthorized transactions, as long as the reviewer is aware of the transaction. Review after the fact cannot prevent unauthorized transactions, but it can uncover them. Maintaining transaction records is essential for sound internal control. Records facilitate reviewing transactions, support the work of internal and external auditors, and form the basis of information reports within a company.

Training enhances internal control by ensuring that staff members know their duties and responsibilities. Providing protective devices such as locked cash drawers, vaults, secured doors, and cameras. Such devices inhibit unauthorized entry and transactions and will be used whenever and wherever feasible.

Providing clerical-proof devices improves internal control by helping to eliminate unintentional errors when transactions are recorded.

Monitoring compliance with the controls, procedures, limits, or other restrictions in place, for example, those placed on personnel involved in investments or those making decisions on underwriting.

4. Information Technology

The reliability, integrity, and availability of critical electronic data are of extreme importance in the company's daily functioning. The company recognizes this and has developed objectives and strategies specifically related to the information technology (hereinafter 'IT') function.

Within these IT strategies, the following matters will be emphasized due to the important impact they have on Operational Risk Management:

User guidelines and training documentation are fully implemented to help ensure that users properly understand the systems they are using, decreasing the risk of errors.

Documented policies and procedures for IT security administration and management are fully implemented covering key requirements such as authentication and

identification, access control, confidentiality, encryption, security management, and virus control.

A Business Continuity and a Disaster Recovery Plan **(hereinafter 'BCP' and 'DRP' respectively)** has been established which clearly states the policies and detailed procedures for recovery in the event of a disaster, which may render the data center or entire building unavailable. Copies of the plan will be stored at an off-site location and distributed to key employees in all relevant departments.

5. Human Resources

The company shall ensure that adequate staffing levels are in place at all times to minimize the occurrence of People Risk. Adequate internal controls as described in the previous section will be established to ensure effective monitoring and control of staffing levels.

To encourage employees to work in a manner that is in the best interests of the company, its Human Resources function will promote a positive work environment and accountability by employees. The following Human Resource Policies will be taken into consideration to mitigate Operational Risk within the Human Resource area of the company:

5.1) The remuneration structure will be aligned with the company's strategic goals. Remuneration policies that reward unacceptable behavior, such as generating short-term profits while deviating from stated policies or exceeding established limits, can weaken the integrity of the company's business processes and will not be permitted.

5.2) Clear work targets and effective performance evaluation.

5.3) Effective procedures for appointment, penalizing, rewarding, promoting, and dismissing.

5.4) Developed policies related to employee career, welfare education, and skills.

5.5) Foster a healthy professional working relationship of mutual respect among employees.

5.6) Effective lines of communication between the company and its employees.

5.7) Well-structured and fair handling of employee problems, in compliance with labour laws and regulations.

6. Risk Identification

The company shall identify the Operational Risks inherent in all material products, activities, processes, and systems. The company shall also ensure that before new

products, activities, processes, and systems are introduced or undertaken, the Operational Risks inherent in them are subject to adequate assessment procedures.

The objective of Operational Risk identification is to ensure that these Risks are identified, contained, managed, and coordinated effectively on a day-to-day basis. Effective risk identification considers both internal factors (such as the company's structure, the nature of its activities, human resources, organizational changes, and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of her objectives.

Human Resource Risk identification requires active participation of departments/ units, through self-assessments. The company must have a focal point at which all non-business risks are managed. This can either be accomplished by direct reporting lines or through regular meetings or facilitated workshops.

The first step in the risk identification process is to identify the main functions in each department/ unit. Each function, in a department/ unit, (e.g. underwriting) must be broken down into various processes (e.g. assessment of the client, risk review, price determination, policy writing...etc.).

Resources linked to these processes must also be identified. Resources will include, but not be limited to, employees, equipment, information technology, and physical custody.

The processes identified must then be mapped and documented.

Once all key processes have been identified and mapped, process owners must be assigned to these processes. Process owners would generally be employees who own or manage a process.

Due to their proximity to the operational performance of the process, the process owners along with their team must identify the potential risks affecting the process, clearly identifying possible operational failures under three categories, people, process, and system.

It is the responsibility of process owners to ensure that loss events are minimized and that Risk Management is made aware of any breakdown in controls.

To identify and assess the Operational Risk inherent in all existing products, activities, processes, and systems, each business unit in the company is required to annually review its key processes and assess each against a menu of potential Operational Risk vulnerabilities.

Identifying New Risk Areas

For all new products, processes, and system/ application implementations, relevant units along with the Risk Management function are required to address the inherent Operational Risks and document relevant controls to mitigate/ minimize these risks.

In rare cases, if the inherent risks are not controllable, a decision will have to be taken to proceed with the product/ process launch based on the risk appetite of the company. However, the risks undertaken in such cases are to be documented to enable a well-thought-out business decision.

As Operational Risk appears to be prevalent where an organization has engaged in a new activity/ product/ service/ system, special attention must be paid by heads of departments to ensure full internal control activities and those procedures are in place before going live.

Requirements for new products/ services/ systems before launch include:

a) Detailed product program/ detailed process map and description;

b) Detailed product/ process risk profile;

c) Profitability projections/cost-benefit analysis;

d) List of inherent and residual risks and required controls for managing the risks; and

e) Use of risk mitigation, their requirements, specifications, etc. Accounting and Finance Requirements:

The following accounting/ financial considerations will be taken when the company conducts new business activities:

i) Determination of how the new product/ process will be accounted for in the books of the company detailing the linkages to accounting and transaction processing policies in place.

ii) Accounts, lines, and categories that will be utilized to capture the various products/processes.

iii) Control requirements on these accounts/ categories to identify errors or suspect transactions.

iv) The delegation of authority for the new product/ process.

Compliance Requirements:

The following compliance considerations will be taken when the company conducts new business activities:

1) Determination of external laws and regulations which have an impact on the product/process documented;

2) Development of controls to ensure compliance;

3) Development of internal policies and procedures which have an impact on the product/process documented;

4) Determine reporting requirements that would be mandated internally (for product management and independent oversight) and externally (to comply with regulatory requirements); and

5) Highlight the specific processes/ data sources that would be utilized to comply with the reporting requirements.

Human Resource Requirements:

The following human resource considerations will be taken when the company conducts new business activities:

a) Determination of resources required for product delivery, control, and monitoring functions; and

b) Highlight the scope for key man risks, if any, and the plans to develop an adequate backup pool for continued product/ process delivery over the long term.

Planning and Budgeting Requirements:

a) Impact of the proposed product/ process on the budgets for current and subsequent years; and

b) Determination of changes in budgets/ plans such as changes in funding costs, changes in pricing structure...etc. All product/ process owners are required to ensure compliance with the above for all new products/ processes and automation projects.

Further, it is the responsibility of the product/ process owners to ensure the review of new proposals by RM to confirm compliance with the above requirements.

RM will ensure the following:

a) Review of new product/ process procedures and process flows;

b) Inclusion of the new products/ processes in the ORSA process; and

c) Ensure that all risks and controls are captured as a part of the documentation requirement adhered to by business/ support units.

7. Operational Risk Assessment Own Risk Self-Assessment (ORSA):

ORSA is a tool that the company will use to assess its operations and activities against a menu of potential Operational Risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the Operational Risk environment.

A key element of the ORSA is the Portfolio Review Process. This process involves a detailed review of Business unit activities as a means to provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of Risk exposures. The Process also contains clear action plans for mitigation/elimination of Risk exposures. Some action plans may relate to risks unique to a specific business line/ product while others may rank risks that cut across business lines/ products (i.e. Resourcing).

In addition, scorecards may be used by the company to allocate economic capital to business lines about performance in managing and controlling various aspects of Operational Risk.

The company shall assess its vulnerability to identified risks. Effective risk assessment allows the company to better understand its risk profile and most effectively target risk management resources.

The company shall conduct an Operational Risk Assessment in line with leading practices pronouncements. Such assessments will consider, but are not restricted to, the following factors below.

From a risk assessment and measurement point of view, Operational Risk must always be assessed at the level of events.

An event in this context may be analyzed in terms of its likelihood (i.e. the probability that an event may occur) and its impact (the consequences or effects if an event does occur).

Whether the company's employees are adequately trained in dealing with its customers. The training program will include specific courses on customer service.

Whether the company's employees are formally trained in underwriting, claims handling, and other Takaful activities.

Whether the company has policies, processes, and procedures to control and/or mitigate material Operational Risks.

The company will periodically review its risk limitation and control strategies and adjust its Operational Risk profile accordingly using appropriate strategies, in light of its overall risk appetite and profile.

Whether record retention policies have been developed/ approved which detail guidelines on the periods for which records/ documents will be retained as well as penalties for non-compliance.

Whether adequate information systems/ analytical techniques/ processes have been implemented to regularly monitor Operational Risk profiles and material exposures to losses.

There will be regular reporting of pertinent information to SM and the BOD that supports the proactive management of Operational Risk.

In addition to the segregation of duties, other internal practices/ physical controls are in place as appropriate to control Operational Risk. Examples of these include maintaining safeguards for access to, and use of, the company assets and records.

Whether the company assesses the Operational Risk inherent in all material products, activities, processes, and systems. In this regard, the company shall ensure that before new products, activities, processes, and systems are introduced or undertaken, the Operational Risk inherent in them is subject to adequate assessment procedures.

Whether documented and approved policies and procedures for valuation of investments/ other assets exist.

Control activities are an integral part of the daily activities of the company. An effective internal control system requires that an appropriate control structure is set up, with control activities defined at every business level.

Whether the company's confirmations for transactions entered into with outside parties are always made in writing. A follow-up process will exist to ensure any outstanding trade confirmations are duly received.

The risk assessment process will be conducted in a workshop where everyone involved in the process has an opportunity to voice their concerns about risks related to the particular business processes and will be facilitated by RM.

Departmental Heads are responsible for undertaking the assessments for their respective units as instructed by RM.

The risk assessment exercise must be conducted regularly, i.e. at least annually for key processes and less frequently for the other processes of the company. Key processes will be identified by the head of each department for purposes of the ORSA.

The users of the Operational Risk System in each department will ensure that the self-assessment process is established and working effectively. The ORSA will capture the company's past and present risk assessments and will make information accessible to

business-level management. The responsibility for the ORSA process should be shared among all employees of the company.

The ORSA process will allow management directly responsible for a business function to:

a) Participate in the assessment of internal control;

b) Evaluate risk;

c) Develop action plans to address identified weaknesses; and

d) Assess the likelihood of achieving the business objectives.

The ORSA may take one of the following meeting formats:

a) Control Based;

b) Process Based;

c) Risk Based; and/or

d) Objective Based.

Process Assessment

RM, as and when required, will assess the adequacy and effectiveness of processes and procedures submitted for review/ comment by the respective business heads of the company and evaluate them to highlight improvements which will consequently help increase external customer satisfaction by way of improved process flows, reduced processing times and reinforcing the corporate view of 'the way things will be done'.

RM shall ensure that: The company maintains robust processes and procedures for the activities conducted by the company's constituents to enhance internal controls; and thereby minimize the possibility of errors/ misappropriations with the consequent impact on financial/ reputation risk; and

The company shall meet minimum standards of control and management disciplines whenever transactions are processed/ services are performed by a constituent.

1. Operational Risk Measurement

Operational Risk measurement must not be a static process that is completed at set times during the year. It must be conducted based on continuous risk and control assessments of the processes of the company.

RM is responsible for maintaining a comprehensive loss events database and adopting more complex tools and procedures, as and when required. Operational Risk measurement will be conducted based on continuous risk and control assessments of the company's processes/ sub-processes and activities.
To obtain a measure of Operational Risk, both the likelihood/ frequency of risk occurrences and the impact or severity of loss must be adequately assessed.

To facilitate the measurement of Operational Risk, the company shall use a variety of tools as discussed in the following sections.
Own Risk Self-Assessment (ORSA) As described in the previous section, The company shall employ an ORSA process through which internal control effectiveness is examined and assessed. RM will employ a system that through the ORSA is conducted and risks measured.

Risk Event Measurement

Risk event measurement will be used to identify and report risks/ losses arising from the Operational Risk Events to develop appropriate action plans to manage Operational Risks consistently and to ensure operational losses are approved appropriately.
Risk event measurement will include:

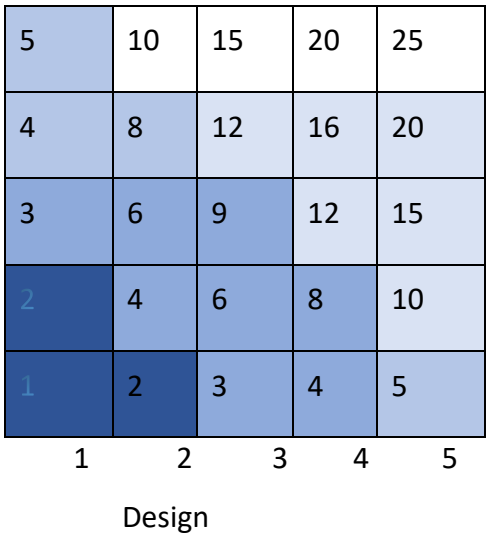
1) Tracking of individual internal event data;
2) Internal loss data linked to current business activities;
3) Frequency and size of loss event; and
4) Analysis of loss event data by business.

RM will establish threshold levels for the collection of lost data. Accordingly, regularly, all process owners will collect and record operational loss event data exceeding

these thresholds, using the format provided by RM

CONTROL RATING

Operational Risk/ Loss events and Near Loss Events above the defined threshold must be sent to RM within 5 business days from the date of the loss event becoming known or reported. RM is responsible for maintaining a comprehensive loss events database.



Legend for control effectiveness

	Very Low
	Low
	Medium
	High
	Very High

Periodically, information relating to deviations of risks and controls from their thresholds and operating losses is to be reported to RM. These statistics and/ or metrics will provide insight into the unit's risk exposure and provide early warnings of near-miss events and possible operational losses.

Risk Likelihood and Impact

To obtain a measure of Operational Risk, both the Likelihood or frequency of risk occurrences and the Impact or severity of loss must be adequately assessed. The likelihood and impact are rated on a scale of 1 to 5, 1 being the lowest, and 5 being the highest. The product of the two gives a measure of the severity of risks faced by a company. As shown in the figure below, a very high score indicates high risk, and a low score, likewise, indicates a low risk.

Operational Risk must be evaluated based on residual risk. Residual risk is the risk that remains in a process after the inherent risk is mitigated by a control system. Thus, if there is a control system in place to mitigate a particular risk, then the likelihood of risk will be adjusted based on the effectiveness of the control system.

Control Design rates how well the control works and Control Performance rates how well the control rating operates. The Design and Performance is also rated on a scale of 1 to 5, 1 being the lowest and 5 being the highest in both Design and Performance (as seen in the below control rating legend). The product of the two will give a measure of Control Effectiveness, or how well the control mitigates and manages the risk.

The risk and control ratings must be further assessed and moderated as part of the consolidation process by the risk monitoring function. These ratings can be used by RM to develop a picture of the overall Operational Risk exposure of the company.

Key Risk Indicators and Key Control Indicators

RM together with each unit head will agree on appropriate risk events/ indicators together with appropriate threshold values representing risk tolerances and limits for their respective groups. Tolerances and limits will be reviewed annually by RM, and approved by the AC.

Key Risk Indicators is an Operational Risk Management tool based on data that indicates the Operational Risk profile of a particular activity/ activities. KRIs will act as an early warning mechanism and will track risks at high-risk points.

RM is responsible for the creation of KRIs for each critical department/ unit in coordination with the concerned head.

RM will ensure that the established KRIs are clearly defined and understood, measurable, and relevant.

Once KRIs are agreed with the critical departments/ units, these will be submitted to the AC for approval.

RM may decide to focus formally on only a few of the identified risks, depending upon the level of priority attached to each risk.

For such risks, a formal log could be maintained by the designated risk owner which will be updated periodically.

The company may not normally monitor KRIs for those activities that are determined to have low likelihood and low severity. However, the company shall monitor the KCIs associated with such activities as the low likelihoods are based on the assumption of effective controls.

Control failures could result in an amendment of the risk likelihood or severity, and lead to an amended assessment of whether KRIs will also be measured.

Controls are preventive in nature; there will be two standard KCIs.

Firstly, an occurrence of a risk event will also represent an instance of that control failing, i.e....., the KRI is also the KCI.

In addition, there may also be cases where the control has failed but has not necessarily resulted in a risk event.

The details below provide examples of risks and their related KRIs and KCIs

Table 2. Examples of Risks and Their Related KRIs and KCIs

Risk	Control	KRI	KCI
Under reserving/ provisioning	Aggregations monitoring system, Actuarial review	Profitability by line of business, Levels of reserves	Aggregation limits exceeded, Actuarial review results
Internal Financial Crime	Authority limits, access controls, internal audits	Near misses, the average size of incidents	Limits exceeded, access breaches, number of audit findings
Inappropriate handling of complaints	Complaints handling procedures	Number of complaints	Staff turnover in complaints, the average time to resolve complaints
Failure of service providers to deliver service levels	Service Level Agreements (SLAs), authorization of new contracts, review of service	Number of 3rd parties used, average size of 3rd party contracts	Number of 3rd party reviews not carried out, SLA breaches

5. Operational Risk Management and Monitoring Guidelines

The company shall ensure that Operational Risk is mitigated and managed continuously using the guidance of the Operational Risk Management Strategy.

It is the responsibility of RM to ensure that steps are undertaken to mitigate Operational Risk at the company-wide level. Service Level Agreements (SLAs), authorization of new contracts, and review of services.

The scope and time horizon for Operational Risk are wide and therefore it is important to prioritize the key risks causing the most exposure to the company, identify which risks will be managed continuously, and those risks to be transferred to third parties (e.g.., Re-Takaful, outsourcing...etc.).

RM will identify the key risks facing a takaful company based on the risk and control ratings and the results of the ORSA process. The key identified Operational Risks must be managed by corrective action stemming from the risk identification and measurement processes. Each identified risk must have an action plan and must be assigned to a process

owner with a specified timeline for completion. The progress of action plans will be monitored by the HRM. The progress of the action plans must be reported to the AC.

RM will continually evaluate and improve its policies and procedures to effectively support operations and undertake risk management and compliance across each product line/ activity/ process. The company's Operational Risk monitoring systems must ensure that both controls and information gathering and reporting are effective and adequate.

It is the responsibility of RM to ensure that regular and adequate monitoring of Operational Risk is conducted on a company-wide level. It is the responsibility of the respective departments/ units to ensure that loss events are minimized and that RM is made aware of any breakdown in controls. RM will be responsible for reviewing all Operational Risk Reports and in case of any concerns will escalate such matters to the AC, as and when required.

6. Operational Risk Reporting

Operational Risk reporting will be an essential part of the internal reporting system and will support the proactive management of Operational Risk.

Regular, objective, and independent reporting on the status and magnitude of Operational Risks faced by the company is crucial in supporting adequate management oversight of the company's Operational Risk.

Reporting on Operational Risk is intended to provide management with regular feedback on the effectiveness of procedures implemented and enable comparison against thresholds of acceptable performance. Examples include:

Results of ORSA Process.

Reports on findings from internal control reviews, conducted by the company's internal and external auditors; IT processing error rates based on volume and turnover of transactions; Downtime of the IT system (or a sub-system) during a month; System breaches per year against money spent on IT security; Reports of testing on, or updates made to the disaster recovery plan and business continuity management plan; Exceptional claims in Takaful business; and Staff turnover.

The HRM will receive regular reports from the company departments which will contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision-making.

The frequency of reporting to RM will be every month or as decided by the company for each division/ department.

Operational Loss and Near Loss Events above a predetermined threshold will be reported within 3 days from occurrence to RM. All events below the established threshold will be reported to RM through regular reporting lines every month.

The scope of information reported to RM from departments/ units will include the following:

i) Changes in the business environment, business practices, and internal control factors;

ii) Risk reduction and risk transfer strategies (e.g., the effect of any expected loss deductions, mitigation and corrective actions on the business line/ event type exposure and/ or losses, cost-benefit analysis of the mitigation actions);

Operational Risk exposures:

• Description of key Operational Risk events and drivers;

• Distribution, trend, and migration of the Operational Risk exposure across business lines; and

• Internal and (where relevant) external loss experience.

• Identification and assessment of vulnerability areas (e.g., ORSA, KCIs, KRIs); and

• Quality improvements in Operational Risk Management and measurement processes and systems.

RM will report periodically to the AC as follows:

i) Operational Loss Events and Near Loss Events will be reported every quarter, highlighting the Operational Risk/ loss event name, description, type of event, and actions taken.

ii) For significant Operational Loss Events RM, will report the event immediately to the AC.

iii) Reporting ORSA results will be on an annual basis for AC which will highlight the gaps revealed through the ORSA process, action plans to address the same, and the implementation status of the agreed plan.

iv) KRI and KCI reporting will be every quarter for AC review.

7. Other Operational Risk Considerations

Outsourcing

Outsourcing is the company's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities continuingly that would normally be undertaken by the regulated entity, now or in the future.

Examples of where outsourcing arrangements include customer sales and relationship management, settlements and processing, IT and data processing.

Outsourcing of activities is one of the approaches The company will employ to transfer some of its risks, management, and compliance in part/in full to a third party/parties. This is accomplished in the following ways:

Outsourcing of some activities allows the company to concentrate on its core business functions. Outsourcing will typically be to a third party or parties, who have more experience in the particular activity, thus giving the company a competitive advantage in managing the related risk.

The company shall ensure that all material outsourcing contracts are identified and that the risks associated with such contracts are adequately controlled.

The company shall require the approval of the local for any material outsourcing agreements.

A contract is considered material where, if it failed in any way, it would pose significant risks to the ongoing operations of the company, its reputation, or the quality of service provided to its customers.

Before a department/ unit enters into an outsourcing arrangement, an ORSA will be carried out by the Compliance/Legal unit, to ensure that the arrangements of the outsourced agent meet the Operational Risk management requirements of the company.

In negotiating a contract with an outsourced contractor or in assessing an existing agreement, The company will consider matters relevant to risk management, including the following:

1) The setting and monitoring of authority limits and referral requirements;

2) The identification and assessment of performance targets;

3) The procedures for evaluation of performance against targets;

4) The provisions for remedial action;

5) The reporting requirements imposed on the outsource contractors (including both content and frequency of reports);

6) The ability of the company's, RM, and its external auditors to obtain access to the outsourced contractors and their records;

7) The protection of intellectual property rights;

8) The protection of customer and firm confidentiality;

9) The adequacy of any guarantees, indemnities, or takaful cover that the outsourced contractor agrees to put in place;

10) The ability of the outsource contractor to provide continuity of business; and

11) The arrangements for change to the outsourcing contract or termination of the contract.

12) The company must retain ultimate responsibility for outsourced services.

13) Risk Management will review all aspects of an outsourcing arrangement and comment upon the same, before its internal approval.

Business Continuity

Disruptions in the company's business can lead to unexpected losses of both a financial and non-financial nature (e.g. data, premises, and reputation). Disruptions may occur as a result of events such as power failure, denial of access to premises or work areas, systems failure (computers, data, building equipment), fire, fraud, and loss of key staff.

All business-critical systems must be covered by full business continuity management procedures and have access to disaster recovery facilities/ plans. The company shall quarterly review the disaster recovery and business continuity plans so that they are consistent with the company's current operations and business strategies.

As part of the Business Continuity Plan, the company shall also analyze the future business and market scenarios and evaluate its dependence on third-party vendors.

The risk of major operational disruptions is incorporated into business continuity planning. Alternate sites will be identified which can act as a backup in case of a disruption. Such an alternate site will be remote enough from the primary business location and will not depend on the same physical infrastructure as the original site. It will be ensured that the alternate site has sufficient data and necessary equipment and systems to recover and maintain critical operations and services for a sufficient period.

The HRM together with the respective unit heads will establish the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to cover severe events outside the company's control, which may make the company's physical, communication, or IT infrastructures inaccessible.

The BCP and DRP will take into account different types of plausible scenarios to which the company may be vulnerable, commensurate with the size and complexity of the company's operations.

Periodic tests will be conducted to assess the operational readiness and effectiveness of BCP and DRP.

Alternative mechanisms will be developed for resuming service, including restoring electronic or physical records, in the event of an outage.

The company shall ensure that suitable backup systems are in place to ensure continuity of operations in the event of an emergency.

The HRM together with the respective department/ unit heads will identify critical business processes for which rapid resumption of service would be essential, and identify the mechanisms for resuming service in the event of an outage.

The Information Technology Department will provide the lead role to ensure that the company's information and the information processing resources under its control are properly protected.

All staff will be familiar with the relevant BCP for their department/ unit.

Legal Risk

Legal risk refers to the possibility of the company's being exposed to loss, penalties, or reputational damage through legal matters such as breaches of laws or regulatory obligations, inadequate contracts, or by changes in law affecting a takaful company.

Legal risk includes, but is not limited to, exposure to fines penalties, or punitive damages resulting from supervisory actions, as well as ordinary damages in civil litigation, related legal costs, and private settlements.

An example of contract inadequacy is where the company's re-takaful arrangements potentially expose the company to significant legal risk where the contract is not valid, binding, or enforceable, or does not clearly set out the respective rights and obligations of the parties, or where a policy document inadequately sets out what exclusions apply.

The company shall use the services of internal and external legal counsel to evaluate the legal risks associated with new and existing products or services and all contractual relationships prior.

Legal Adviser is required to be informed of all changes in the legal system that affect the company and communicate them to the company management. Legal Adviser must identify and document all legal risks in the company's transactions.

Legal Adviser must review all legal contracts, ensuring such contracts are in the company's best interests.

The Legal Adviser will regularly (quarterly) update the database as and when new risks are identified or new laws are enacted. The legal risk database must be forwarded to RM.