GUEVENT INSURANCE BROKER CORP.

**Get Insured, Be COvered. GIBCO, At Your Service!**

# RISK MANUAL

# 2025

*The information contained within this document is HIGHLY CONFIDENTIAL and unauthorized disclosure is prohibited. Failure to observe Guevent Insurance Broker, Corp. policy regarding proprietary information can result in a disciplinary action, including dismissal, and can subject you and/or third parties to legal liability.*

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

# TABLE OF CONTENTS



The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

# RISK MANUAL

## 1.0 INTRODUCTION

This Risk Manual provides the framework on the Risk Management and Assessment of GUEVENT INSURANCE BROKER CORP.'s ("GIBCO") operations and internal/external processes as required by the Insurance Commission, in compliance with industry regulations, standards and risk management. It serves as guide to the Board of Directors, Executive Committee and Management Committee. Effective risk management enables GIBCO to identify the potential risks and operational weaknesses in order to significantly reduce its exposure to errors, omissions, and financial losses. The risk assessment process is essential in ensuring that GIBCO's operations remain aligned with its Mission, Vision and Core Values.

### 1.1 Purpose

- Define scope and role of Risk and Corporate Governance Committee of the Board.
- Ensure transparent communication of risk assessments and management.
- Promote risk-based auditing to address organizational risks effectively.

### 1.2 Risk Assessment and Management Scope

Risk assessment and management cover financial, operational, compliance, and IT systems, ensuring that policies, procedures, and controls are effective and aligned with corporate objectives while reducing the likelihood of its exposure to errors, omissions, and financial losses.

## 2.0 ORGANIZATIONAL STRUCTURE

GIBCO operates with a clear organizational structure to facilitate effective risk management.

The Chief Executive Officer ("CEO") provides strategic oversight, while the Internal Audit and Risk Officer (IAR) is responsible for identifying, assessing, and mitigating risks across all business functions. Close collaboration between Internal Business Units, External Business Units, Business Development, Claims, Information Technology (IT), Human Resources (HR), and Finance Department Heads ensures alignment with risk management objectives and regulatory requirements. The Audit and Risk Officer reports directly to the CEO/President providing independent risk oversight and ensure accountability at the executive level.

## 3.0 RISK AND CORPORATE GOVERNANCE FRAMEWORK

Risk and corporate governance establish the foundational structure to ensure the independence, accountability, and effectiveness of the risk function. It involves the alignment of Board- level Risk Committee and internal audit and risk activities with corporate objectives, regulatory requirements, and best practices. This framework aims to provide clear oversight and communication channels among risk functions, Audit and Risk Management Committee, and the Board of Directors.

### 3.1 Reporting Structure

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

1. **Chairperson/ Head** – Must possess appropriate expertise and skills to effectively lead the Committee.
2. **Member** – A non-executive director, preferably with knowledge or experience in compliance, risk management, or governance.
3. **Member** – A non-executive director who can provide independent oversight and contribute to the Committee's mandate.

*The updated list of committee members is provided in **Annex I** of this Manual.*

3.1.1.2 Role of the Risk Committee:

a. Advises the board on enterprise risks across financial, operational, legal, reputational, and strategic domains, as well as risk implications of major strategic decisions.
b. Support Audit & Risk Committee by reviewing audit findings related to the company's risk exposures and ensure timely remediation.

3.1.1.3 Role of Board of Directors:

a. Provides strategic oversight to ensure risk functions are effectively integrated into corporate governance.
b. Receives periodic updates on audit activities, critical findings, and risk assessments.

### 3.1.2 Audit and Risk Reporting Lines

3.1.2.1 The Audit and Risk Officer reports operationally to the President and has dotted-line reporting to the Risk and Corporate Governance Committee of the Board of Directors.

3.1.2.2 This dual reporting structure ensures operational alignment while preserving the independence necessary for objective audits.

## 4 RISK MANAGEMENT

**4.1** **Risk Management Policy Statement.** GIBCO is committed to identifying, assessing, and managing risks to protect clients' interests, maintain regulatory compliance, and safeguard the company's reputation. We evaluate supplier risks to ensure they are reliable, compliant, and do not pose a threat to our operations or reputation.

**4.2** **Risk Categories**

The risk categories outlined below serve to raise organizational awareness of potential risks within each category. These promote a systematic approach to risk identification and assessment, ensure consistent use of terminology across the company, and facilitate proper categorization of risks to support effective evaluation and response strategies.

Risk categories include:

**4.2.1** **Operational Risks**: Risks related to internal processes, technology, and human error.
**4.2.2** **Financial Risks**: Risks associated with market fluctuations, credit exposure, and liquidity.
**4.2.3** **External Risks**: Risk associated with client management and interaction with principal(supplier).
**4.2.4** **Legal Risks**: Risks arising from non-compliance with laws, regulations, and industry standards.
**4.2.5** **Reputational Risks**: Risks affecting the company's reputation and brand image.
**4.2.6** **Environmental, Social, and Governance (ESG) Risks:** These include risks arising from environmental sustainability, social impacts (e.g., labor practices, diversity), and governance integrity (e.g., corruption, board oversight). ESG risk factors are considered in strategic planning and regulatory compliance. *(Tools in **Annex IX**: ESG Risk Criteria and Assessment Template)*
**4.2.7** **Emerging Risks:** Risks related to emerging technologies like Artificial Intelligence (AI), cybersecurity, and other relevant advancements.

**4.3** **Risk Management Framework**


The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

4.3.1 **Risk/Hazard Identification**: The company's risk identification process is designed to ensure that all material risks affecting the company, and its entities are properly identified. During this stage, risks related to client services, regulatory changes, market fluctuations, and operational processes are identified and documented.

To support effective risk identification, employees undergo continuous training aimed at enhancing their ability to detect and report risks across the company's operations.

Risk identification within each department's operations is conducted by evaluating each Key Performance Area (KPA) as defined by the Management Committee. Additionally, risks and hazards are identified by analyzing specific activities and situations commonly encountered or performed by employees.

In terms of client services, the submission of required documents and Know-Your-Client (KYC) procedures shall strictly follow the established manual and the prescribed list of requirements. For any client or transaction identified as a covered or suspicious, the appropriate protocols for such cases shall be duly observed in accordance with applicable regulations and internal policies.

4.3.2 **Risk Evaluation**: Risks are evaluated based on their **likelihood** of occurrence and their **potential impact** on the company's objectives, clients, and regulatory obligations. Departmental operations are assessed using the company's Risk Assessment Criteria, which supports the prioritization of risks that require immediate corrective action, close monitoring, or escalation to the Management Committee or the Board of Directors.

This stage encompasses all significant risks identified during the Risk Identification phase, including operational, financial, regulatory, and reputational exposures—particularly those linked to **new products, services, or markets**.

GIBCO uses a **Risk Evaluation Matrix** to systematically assess each identified risk across all business units. The matrix categorizes risk levels by combining impact and likelihood ratings, enabling Internal Audit and the relevant committees to focus on critical exposures that could result in regulatory penalties, financial losses, or reputational damage. (*Refer to Annex III – Sample Risk Evaluation Matrix for Insurance Broker Operations* for the detailed matrix and examples of assessed risks.)

4.3.3 **Risk Control/Response**: Appropriate risk mitigation strategies, risk transfer mechanisms, and risk acceptance criteria are established to address identified risks in a structured and effective manner. The control or response measures to be implemented shall be determined based on the severity level of the risk as assessed through the established Risk Assessment Criteria.

**Risk Mitigation Strategies** include the following:

**Segregation of Duties:**

- Assigning distinct responsibilities to different individuals or departments to prevent conflicts of interest, errors, and fraudulent activities.

**Internal Controls:**
Implementing control activities such as authorization procedures, reconciliations, approvals, and physical safeguards to secure access to assets and ensure compliance with policies and regulations.

**Business Continuity Planning:**
Developing and maintaining robust business continuity plans and disaster recovery strategies to minimize disruptions, protect critical business functions, and ensure the continuity of operations in the event of emergencies or unforeseen events.

In support of our sustainability initiatives, our Business Continuity Planning (BCP), as outlined in the Guevent BCP Manual, proactively addresses critical risk areas including economic volatility, climate change, cybersecurity threats, technological advancements, geopolitical instability, and supply chain disruptions.

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

Our BCP is structured around five essential pillars to ensure operational continuity and organizational resilience:

1. Equipment – Ensuring availability, maintenance, and rapid replacement of essential hardware and tools.
2. Data – Safeguarding data integrity, security, and accessibility through robust backup and recovery protocols.
3. Staff – Protecting personnel welfare, enabling remote work capabilities, and maintaining knowledge continuity.
4. Premises – Securing alternative workspaces and maintaining infrastructure adaptability in the face of environmental or man-made disruptions.
5. Supply Chain Resilience – Building flexible and diversified supply networks to withstand external shocks and maintain service delivery.

This integrated approach underscores our commitment to both operational resilience and long-term sustainability.

**4.3.4 Risk Monitoring and Review**: The ongoing monitoring of risks and periodic reviews ensure the effectiveness of risk management measures.

### 4.4 Hazard Identification, Risk Assessment and Control (HIRAC) Form

The HIRAC Form facilitates the effective identification and selection of risks by specifying those that GIBCO intends to acquire, avoid, retain, or remove. It also outlines the measures in place to guide management activities, as well as the procedures for monitoring and escalation.
Risk management strategies for each category are detailed in the relevant policies and corresponding guidelines.
The HIRAC Form incorporates Risk Assessment Criteria, enabling the Committee to determine the level of exposure GIBCO has to each identified risk and to identify the appropriate control or mitigation measures required.

*(Attached herewith are the Risk Assessment Criteria Matrix and a sample HIRAC Form for reference.)*

### 4.5 Third-Party Risk Management

GIBCO shall implement robust third-party risk procedures including:

- Comprehensive vendor due diligence (financials, legal, cybersecurity, compliance, etc.)
- Contractual clauses for risk compliance
- Ongoing monitoring of vendor performance and incidents
- Evaluation of principal concentration risk, especially for insurer relationships

*(Refer to **Annex VIII**: Third-Party Risk Assessment Checklist & Monitoring Log)*

## 5 COMPLIANCE AND REGULATORY REQUIREMENTS

GIBCO complies with all relevant laws, regulations, and industry standards governing insurance broker operations, including but not limited to:

- Insurance Regulatory Authority guidelines
- Data protection laws
- Anti-money laundering regulations and know-your-customer (KYC) regulations
- Compliance Officer for AMLA and Certificate of Registration shall be updated every 2 years or if there be a change in the officer.
- Market conduct and consumer protection standards

## 6 INTERNAL CONTROLS

GIBCO maintains a strong internal control environment characterized by the following key elements:

**Tone at the Top:**

- The Management Committee (MANCOM) sets the tone for ethical behavior, accountability, and strict adherence to internal control policies and procedures.

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

This leadership fosters a culture that reflects and upholds the Mission, Vision, and Core Values of GIBCO.

**Policies and Procedures:**

- Documented policies, procedures, and guidelines are established to govern key business processes, mitigate risks, and ensure compliance with regulatory requirements.

**Monitoring and Review:**

- Regular monitoring, reviews, and assessments of internal controls are conducted to identify weaknesses, address deficiencies, and enhance control effectiveness.

**Reporting and Escalation:**

- Mechanisms are established to ensure the prompt reporting of control deficiencies, irregularities, and potential fraud incidents promptly to management, the Board of Directors, and relevant authorities for appropriate investigation and remediation.

**6.1 Incident Management and Post-Mortem Analysis**

GIBCO adopts a formal incident management process to detect, report, investigate, contain, and recover from operational, regulatory, or reputational events. All significant incidents shall undergo a structured post-mortem review to determine root causes and develop Corrective and Preventive Actions (CAPAs). *(Refer to **Annex VI**: Incident Management Protocol and Post-Mortem Template.)*

**6.1.1** GIBCO maintains a defined risk appetite that outlines acceptable levels of exposure across financial, operational, reputational, and compliance areas. This serves as a guide for decision-making, ensuring alignment with the company's objectives and regulatory obligations. *(Refer to Annex II – Risk Appetite Statement for details.)*

**6.1.2** The Audit and Risk Officer shall coordinate with each department to ensure ownership and accountability of specific risk categories. A departmental risk responsibility matrix shall be maintained and periodically reviewed to clarify roles in risk identification, mitigation, control implementation, and reporting. *(Refer to Annex V – Departmental Risk Ownership Matrix.)*

## 7 MONITORING AND REPORTING

Risk activities are monitored as follows:

**Performance Measures:**

- **Key performance indicators (KPIs)** are tracked to measure the effectiveness of risk management and audit processes.
- In terms of employee output per department, performance monitoring is conducted through:

  (a) Weekly check-ins with functional teams and department heads to track incremental progress against the team's action plan; and
  (b) Monthly progress reports prepared by Human Resources, which highlight departmental milestones, achievements, and confidence levels, and are presented to both department heads and the CEO.

- **Key Result Areas (KRA)**

  These include:
  (a) Strategic Leadership,
  (b) Business Development,
  (c) Financial Performance,
  (d) Operational Excellence, and
  (e) People Development.

  Each KRAs is supported by Key Performance Areas (KPAs) that define the specific tasks and responsibilities to be assessed. Management Committee (MANCOM) uses KPAs to evaluate departmental and individual performance.

  Department-specific KPAs are linked to the KRAs and are accompanied by measurable metrics that are monitored monthly by HR to track progress.

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

- **Objective Key Results (OKR)**
  OKRs are used to monitor the progress of objectives to ensure accountability and effective resolution of identified risks and audit findings.
- A Risk Management Information System (RMIS) will be explored to support automated risk tracking, analytics, control effectiveness monitoring, and centralized documentation.
- Data quality, timeliness, and integrity are essential for reliable risk KPIs and OKRs. Risk data shall be validated quarterly before submission to the Board. (*Link to **Annex VII**: RMIS and Data Integrity Tools.)*

**Management Reports:**
Periodic management reports and documentations are made to summarize key risk metrics, findings, and compliance status for Management Committee and the Board of Directors.

**Board Reporting:**
Comprehensive reports are regularly submitted to the Board of Directors, Executive Committee, and other governance bodies to communicate significant risks, results of risk assessments, and corresponding recommendations. Quarterly reports are required to ensure that risk oversight remains timely and aligned with business operations. In addition, preferred meetings shall be scheduled by the Risk and Governance Committee Chair if deemed necessary to address emerging issues or conduct in-depth reviews.

These reports aim to support informed decision-making, reinforce oversight responsibilities, and ensure alignment with the organization's strategic objectives.

**Key risks, assessment results, and recommendations are submitted to the Board of Directors and relevant committees to support informed decisions and effective oversight. Independent directors play a critical role in ensuring objectivity, challenge assumptions, and uphold strong risk governance.**

## 8 TRAINING AND AWARENESS

GIBCO places a high priority on employee training and awareness initiatives to foster a culture of risk awareness, ethical behavior, and compliance with policies and procedures at all levels of the organization.

Training programs cover a wide range of topics, including:
- **Risk Management Fundamentals**: Covers the core principles of identifying, assessing, mitigating, and monitoring risks across operations.
- **Internal Control Awareness**: Emphasizes the role of internal controls, proper segregation of duties, and adherence to compliance protocols
- **Compliance Training**: Educates employees on relevant laws, regulations, and industry standards governing insurance broker operations, including Anti-Money Laundering (AML), data protection, and market conduct regulations.
- **Audit Awareness**: Provides insight into the audit process, outlines employee responsibilities, and reinforces the value of transparency and collaboration during audits and reviews.

Training programs and workshops are scheduled annually by the HR department and conducted through a combination of online and face-to-face seminars and activities.

Employees of GIBCO are likewise mandated to attend agency-led seminars, such as AMLC webinars, to further equip themselves with knowledge essential to the Company's operations.

## 9 CONTINUOUS IMPROVEMENT

GIBCO is committed to continuous improvement in its risk management and audit processes driven by a culture of innovation, learning, and accountability,
Risk management and audit frameworks are regularly evaluated and enhanced based on stakeholder feedback, emerging risk trends, and insights gained from past incidents.

Key elements of the continuous improvement process include:

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

- **Feedback Mechanisms**: Soliciting feedback from stakeholders, including employees, customers, regulators, and business partners, to identify areas for improvement and proactively address concerns.
- **Lessons Learned**: Capturing and documenting insights learned from past incidents, audit findings, and industry developments to inform risk management strategies, policies, and procedures.
- **Risk Reviews**: Conducting periodic reviews and updates of risk registers, control frameworks, and audit plans to ensure alignment with evolving business environment, emerging risks, and regulatory requirements.
  The report, together with the updated risk register file, is submitted on a quarterly basis. Additionally, interim updates may be provided upon request or as needed, particularly in cases where new risks are identified or urgent issues require immediate attention and escalation.
- **Best Practices**: Benchmarking against industry best practices, standards, and frameworks to identify opportunities for enhancing risk management effectiveness, operational efficiency, and governance practices.
- **Strategic Risk Integration and Foresight Planning**: GIBCO integrates scenario planning, environmental scanning, and cross-functional risk workshops (refer to Annex III) into its risk management framework. These tools help anticipate high-impact, low-likelihood risks and inform strategic decisions. Risk assessments are embedded into major business initiatives, and risk-adjusted performance tracking is aligned with existing monitoring tools (e.g., audit tracker, corrective action logs), which will be continuously enhanced to support key risk indicators. *(Templates and logs are provided in Annex IV: Risk Engagement Tools.)*

## 10 REVIEW OF MANUAL

- The Committee shall conduct a **bi-annual review** and assessment of the adequacy of the Risk Manual to include development in legislation, market and/or best practices, group strategy, organization, and propose any change as may be deemed necessary for the Board's approval.
- An external, independent assurance review of the enterprise risk management framework shall be conducted at least every three years by a qualified risk audit firm or independent consultant.

## 11 EFFECTIVITY

This Manual supported by the Audit and Risk Management Committee shall take effect immediately upon approval by the Board of Directors.

**DOCUMENT HISTORY**

| Revision No. | Effectivity Date | Description of Revision | Section | Author |
|---|---|---|---|---|
| | | | | |

**DISTRIBUTION/ ACCESS LIST**

| Division / Department – Position | Type of Copy | Type of Accessibility |
|---|---|---|
| All | Soft Copy | Read Only |
| Document Controller | Soft Copy & Hard Copy | Full Access |

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

Annex I – Composition of the Risk Management Committee

(As referenced in Section 3.1.1 of this Manual)
The duly appointed Audit Committee members as of December 2023 are as follows:

| Name | Position | Designation/Role in the Committee | Background/Expertise |
|---|---|---|---|
| Eric Lim | Independent Director | Chairperson/ Head | Risk and Governance expert |
| Felix Uy | Independent Director | Member | CPA, extensive experience in audit and risk |
| Christine Natalie Joyce D. Guevara | Director | Member | |
| Carmen Rita M. Bautista | Director | Member | |
| Monica Pauline G. Dela Cruz | Director | Member | |

Note: This composition is updated as of 25 July 2025 and subject to change based on Board resolutions and appointments.

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

**Annex II – Risk Appetite Statement**

(As referred to in Section 6.1.1 of this Manual)

**RISK APPETITE STATEMENT**

GIBCO adopts a **prudent and risk-aware approach** to conducting its operations, ensuring that risks are understood, monitored, and managed within acceptable levels that support the achievement of its strategic and operational objectives. The company acknowledges that, as an insurance broker, its role involves safeguarding client interests, ensuring regulatory compliance, and preserving trust and reputation in a competitive and highly regulated environment.

**1 Risk Appetite Overview**

GIBCO's **risk appetite** defines the **types and levels of risk the organization is willing to accept, avoid, or mitigate** in pursuit of its objectives. It provides a guide for decision-making, resource allocation, and risk response strategies across all departments. The company's appetite varies by risk category, as outlined below:

**2 Acceptable Risk Levels by Category**

- **Financial Risk Appetite**
  - **Low to Moderate.** GIBCO has a limited tolerance for financial losses and maintains robust internal controls to prevent fraud, misappropriation, or operational inefficiencies that may result in material financial loss. A minor level of financial deviation may be acceptable in pursuit of business development or technology investment, provided they are thoroughly assessed and approved.
- **Operational Risk Appetite**
  - **Low.** GIBCO maintains a low appetite for operational failures, including process lapses, system downtime, or client servicing delays. It prioritizes continuity, process efficiency, and regulatory compliance in its operations. Any risk that could significantly disrupt service delivery or client trust is considered unacceptable.
- **Compliance and Legal Risk Appetite**
  - **Zero Tolerance.** GIBCO does not tolerate non-compliance with legal, regulatory, or industry standards, particularly in areas concerning Anti-Money Laundering (AML), Data Privacy, Know-Your-Customer (KYC), and licensing. Full compliance is non-negotiable to protect the company from penalties, license revocation, or reputational damage.
- **Reputational Risk Appetite**
  - **Very Low.** As a client-facing entity in the insurance industry, GIBCO places utmost importance on its reputation. Any risk that may negatively impact client trust, brand integrity, or stakeholder confidence is deemed unacceptable.
- **Strategic and Business Development Risk Appetite**
  - **Moderate.** GIBCO is open to exploring new markets, products, or technologies, provided risks are managed within clear parameters and proper due diligence is conducted. Strategic initiatives should align with the company's mission and not compromise core compliance, service quality, or financial stability.

**3 Risk Tolerance Thresholds (Examples)**

| Risk Type | Acceptable Threshold |
|---|---|
| **Financial Loss** | Not exceeding 1% of annual revenue per incident |
| **Regulatory Penalties** | Zero tolerance; all violations to be escalated immediately |
| **System Downtime** | Not exceeding 1 hour per quarter for core systems |
| **Client Complaints** | Not exceeding 3% of monthly active clients |
| **Data Privacy Breach** | Zero tolerance |

**4 Governance and Review**

This Risk Appetite Statement shall be reviewed annually or as necessary by the **Audit and Risk Officer** and approved by the **Board of Directors** to ensure alignment with evolving regulatory, operational, and market conditions. All department heads shall ensure that strategies and decisions are consistently aligned with GIBCO's defined risk appetite.

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

**ANNEX III - Sample Risk Evaluation Matrix**

(As referenced in Section 6.1.1 of this Manual)

Sample Risk Assessment Matrix – Insurance Broker Context

| Impact ↓ / Likelihood → | 5 (Almost Certain) | 4 (Likely) | 3 (Possible) | 2 (Unlikely) | 1 (Rare) |
|---|---|---|---|---|---|
| 5 (Severe) | Data breach exposing client info<br>Impact: High reputational and regulatory risk<br>Risk Owner: IT Head | | | | |
| 4 (Major) | | **Failure to comply with AMLA requirements**<br>Impact: Regulatory penalties<br>Risk Owner: Compliance Officer | | | |
| 3 (Moderate) | | | **Delayed submission of quarterly report to Insurance Commission**<br>Impact: Reputational and compliance impact<br>Risk Owner: Internal Audit | | |
| 2 (Minor) | | | | **Client dissatisfaction due to delayed policy endorsement**<br>Risk Owner: External Business Unit | |
| 1 (Insignificant) | | | | | Internal memo routing delays<br>Minimal impact<br>Risk Owner: HR/Admin |

**Explanation of Flow**

1. **Risks are first identified** from internal operations or compliance requirements (e.g., via audit, walkthroughs, incident reports).
2. Each risk is **plotted based on impact (vertical)** and **likelihood (horizontal)**.
3. Items in red or orange zones (Severe/Almost Certain or Major/Likely) are flagged for **Board-level or MANCOM attention**.

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

4. Each risk item includes:
    - **Risk event/issue**
    - **Nature of impact** (financial, compliance, reputational, operational)
    - **Assigned risk owner** (to monitor or respond)
5. **Treatment plans** are then proposed based on the matrix level (see 4.3.3).

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

## ANNEX IV RISK ENGAGEMENT TOOLS

(As referred to in Section 9 of this Manual)

**1. Mandate Scenario Planning and Stress Testing**

**Purpose:** Test the organization's resilience under extreme but plausible conditions.

**Execution Steps:**

- Identify major risk categories (e.g., Financial, Operational, Regulatory, External).
- Develop at least two scenarios per category annually (e.g., recession, cyberattack).
- Use a scoring method for **impact vs likelihood** and test controls and mitigations.

**Example Table: Scenario Planning Matrix**

| Risk Category | Scenario Description | Likelihood | Impact | Control Measures | Gaps Identified | Action Plan |
|---|---|---|---|---|---|---|
| Financial | Major economic downturn | Medium | High | Cost control, reserve funds | No buffer funds for 3 months | Build 6-month reserve |
| Cybersecurity | Widespread ransomware attack | Low | Very High | Cloud backup, endpoint security | Training gap in branch ops | Conduct drills, staff orientation |

**Responsibility:** Risk Officer in coordination with IT, Finance, and Operations.

**2. Formalize Environmental Scanning**

**Purpose:** Anticipate changes in external threats through proactive monitoring.

**Execution Steps:**

- Assign focal persons per department to contribute to a **monthly environmental scan report**.
- Use sources like BSP, SEC bulletins, economic reports, industry forums, and international alerts.
- Summarize insights quarterly in a short environmental risk bulletin.

**Example: Environmental Scanning Log Template**

| Date | Source | Topic Monitored | Relevance to GIBCO | Action Required |
|---|---|---|---|---|
| May 2025 | BSP Circular 1189 | New capital requirement for brokers | May affect capital adequacy | Coordinate with Finance |
| June 2025 | PAGASA Advisory | Above-normal typhoon frequency | Risk to office ops/disruption | Revise BCP protocols |

**Responsibility:** Compliance or Risk Department compiles reports for the Audit Committee.

**3. Cross-Functional Risk Workshops**

**Purpose:** Encourage collective risk ownership across departments.

**Execution Steps:**

- Conduct **bi-annual risk workshops**.
- Invite heads from key departments (e.g., Claims, Underwriting, IT, HR).
- Use structured templates to identify risks from each unit and cross-check for dependencies.

**Example: Cross-Functional Risk Map**

| Department | Key Risks Identified | Dependencies with Other Units | Mitigation Strategy | Timeline | Responsible |
|---|---|---|---|---|---|
| IT | Legacy systems | Claims (system downtime) | Upgrade plan Q3 | Dec 2025 | IT Head |
| Claims | Delayed settlements | Finance (funding release) | Improve process flow | Sep 2025 | Claims Head |

**Output:** A consolidated risk register with inputs from all teams, submitted with the quarterly report.

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

**Annex V – Departmental Risk Ownership Matrix**

(As referred to in Section 6.1.2 of this Manual)

| Department | Risk Focus Area | Key Responsibilities | Reports To |
|---|---|---|---|
| Operations | Service continuity, vendor risk | Identify process bottlenecks, ensure BCP protocols | ARO → CEO |
| Finance | Financial controls, misstatements | Maintain integrity of financial reporting, escalate discrepancies | ARO → CEO |
| Claims | Fraud, SLA delays | Monitor claim patterns, flag anomalies, support investigations | ARO → CEO |
| IT | Cybersecurity, data privacy | Implement access controls, report incidents | ARO → CEO |
| Compliance | Regulatory non-compliance, licensing | Monitor circulars, update management, ensure timely filings | ARO → CEO |
| ARO (Central Role) | Enterprise risk coordination, consolidation | Maintain ERM tools, consolidate reports, escalate critical risks | Board, CEO, Committees |

This matrix will be updated at least annually or upon major organizational changes.
The HR department is **not included** in the matrix since KRAs/OKRs are tracked separately.

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

**Annex VI: Incident Management Protocol and Post-Mortem Tools**
(As referenced in Section 6.1 of this Manual)

**A. Incident Management Protocol Table**

| Step | Description | Responsible Person/Unit | Timeline |
|---|---|---|---|
| 1 | **Incident Detection**: Employee or system detects an unusual event, breach, failure, or non-compliance. | Any staff / system alert | Immediately |
| 2 | **Initial Reporting**: Complete Incident Report Form and submit to Audit and Risk Officer (ARO). | Department Head / Reporter | Within 1 working day |
| 3 | **Preliminary Assessment**: Assess the impact, urgency, and need for escalation. | ARO + Concerned Department | Within 1 working day |
| 4 | **Escalation**: Notify the CEO, Committee, or regulators if high risk or regulated event. | ARO | Within 2 days (or earlier as required) |
| 5 | **Investigation**: Conduct fact-finding, root cause analysis, and gather supporting documents. | ARO + Assigned Team | Within 3–5 working days |
| 6 | **Containment & Recovery**: Implement immediate actions to prevent further damage and restore normal operations. | Concerned Department | ASAP, with updates |
| 7 | **Documentation**: Record incident details, findings, and recovery measures. | ARO | Ongoing |
| 8 | **Post-Mortem Review**: Hold a structured review meeting to identify lessons learned and update controls or processes. | ARO + Concerned Units | Within 7–10 days post-incident |
| 9 | **Corrective & Preventive Actions (CAPA)**: Develop and assign action plans. Update risk register if applicable. | ARO + Process Owner | Within 10–15 days |
| 10 | **Monitoring**: Track CAPA implementation using existing tools (e.g., Audit Recommendation Tracker or Corrective Action Log). | ARO | Ongoing |

**B. Sample Incident Report Form**

| Field | Details |
|---|---|
| Incident Title | |
| Date & Time of Occurrence | |
| Reporting Person | |
| Department / Unit | |
| Description of Incident | |
| Impact Type | ☐ Operational ☐ Compliance ☐ Reputational ☐ Financial |
| Initial Actions Taken | |
| Person Notified | |
| Attachments (if any) | |

**C. Sample Post-Mortem Review Summary Template**

| Item | Details |
|---|---|
| Incident Reference | |
| Summary of Incident | |
| Root Cause(s) | |
| Immediate Containment Measures | |
| Corrective Actions | |
| Preventive Measures | |
| Responsible Person(s) | |
| Target Dates | |
| Risk Register Updated? | ☐ Yes ☐ No |
| Policy/Procedure Updates Needed? | ☐ Yes ☐ No |
| Lessons Learned | |

**D. Corrective and Preventive Action Tracker (linked with existing ARTS)**

| Finding | Action | Responsible | Deadline | Status | Remarks |
|---|---|---|---|---|---|
| Root cause of data entry error in claims | Add system validation rules | IT Head | July 30, 2025 | In Progress | Testing UAT |
| Failure to escalate KYC delay | Update escalation policy and train staff | Compliance | Aug 15, 2025 | Not Started | Orientation scheduled |

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

**Annex VII – RMIS and Data Integrity Tools**
(As referenced in Section 7 of this Manual)

- Sample RMIS Dashboard (fields: risk ID, owner, rating, status, control owner, next review)

| Risk ID | Risk Owner | Risk Title | Risk Rating | Status | Control Owner | Next Review Date | Last Updated |
|---|---|---|---|---|---|---|---|
| RSK-001 | Claims Dept | Delayed Claims Payout | High | Open | IT Manager | Aug 15, 2025 | June 15, 2025 |
| RSK-002 | Finance | Liquidity Shortfall | Medium | Monitoring | CFO | Sept 5, 2025 | June 1, 2025 |

- Data Validation Log Template (field: data type, frequency, validator, notes)

| Data Type | Validation Frequency | Validator | Method Used | Validation Result | Remarks |
|---|---|---|---|---|---|
| KPI – Audit Findings | Quarterly | ARO | Manual cross-check | Validated | Reviewed with IA Head |
| Risk Register Entries | Quarterly | Risk Committee | System report + audit log | Validated | Aligned with Risk Matrix |
| Vendor Risk Ratings | Semi-Annually | Compliance Team | Third-party score + checklist | Pending Review | Awaiting vendor updates |

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

**Annex VIII – Third-Party Risk Management Tools**
(As referenced in Section 4.5 of this Manual)

- Vendor Due Diligence Checklist (legal docs, financials, cybersecurity, AML/KYC compliance)
- Vendor Risk Monitoring Log (vendor name, risk rating, incidents logged, contract expiry)

| Requirement | Compliant (Y/N) | Remarks / Notes |
|---|---|---|
| Valid Business Permit / Mayor's Permit | Yes | Updated for FY 2025 |
| Latest Audited Financial Statement | Yes | FY 2024 submitted |
| Cybersecurity Controls / Certifications | No | SOC 2 compliance pending |
| AML / KYC Policy Disclosure | Yes | AML policy reviewed Mar 2025 |
| Data Privacy Consent / NDAs | Yes | On file, signed Jan 2025 |

| Vendor Name | Risk Rating | Issues / Incidents Logged | Performance Notes | Contract Expiry |
|---|---|---|---|---|
| InsureCo | Medium | 1 delay (Q1 2025) | Improved after escalation | Dec 31, 2025 |
| ABC IT Services | High | Data breach flagged (Feb 2025) | Under remediation review | Aug 30, 2025 |

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.

**ANNEX IX – ESG RISK CRITERIA AND ASSESSMENT TEMPLATE**
(As referenced in Section 4.2.6 of this Manual)

- ESG Risk Matrix (e.g., climate exposure, labor issues, governance gaps)
- ESG Policy Compliance Tracker (criteria, responsible dept, last review, status)

| Risk Area | Specific Concern | Severity | Likelihood | Impact Summary | Response Plan |
|---|---|---|---|---|---|
| Climate Exposure | Office in flood zone | Medium | Likely | Operations halted post-storm | Relocation/BCP |
| Labor Practices | No DEI policy | High | Moderate | Reputation & legal exposure | Develop & roll out HR DEI |
| Governance Gaps | Weak conflict-of-interest rules | Medium | High | Compliance risk | Policy update + training |

| ESG Criterion | Responsible Department | Last Reviewed | Status | Next Review Date |
|---|---|---|---|---|
| Anti-Corruption Policy | Compliance | May 2024 | In Progress | Nov 2025 |
| Diversity & Inclusion | HR | Jan 2024 | Compliant | Jan 2026 |
| Environmental Compliance | Facilities & Admin | Feb 2023 | Needs Update | Aug 2025 |

The information contained in this document is a property of GIBCO. It may not be copied, reproduced, released to any third party, or used in any other way without the express prior written consent of the owner of this document.