2026

INSURANCE COMMISSION
OF THE BAHAMAS

GUIDANCE FRAMEWORK FOR THE INTERNAL AUDIT FUNCTION

Silk Cotton House, Prospect Ridge Road - P.O. Box N-4844 - New Providence, The Bahamas
Tel: (242) 603-4183 - Email: info@icb.gov.bs - Website: www.icb.gov.bs

FOLLOW US

@INSURANCECOMMISSIONBAH

Table of Contents

About the Insurance Commission of The Bahamas

The Insurance Commission of The Bahamas ("The Commission") was established on July 2, 2009, under The Insurance Act 2005, Chapter 347, and is responsible for the regulation of all insurance activity in and through The Bahamas.

In its role as both the prudential and market conduct regulator, its purpose is to ensure a sound and stable insurance marketplace and consumer confidence in the insurance industry.

The mandate of the Commission includes:

- Administration of the Insurance Act, 2005 and the 2009 External Insurance Act
- Insurance market surveillance
- Promotion and encouragement of sound and prudent insurance management and business practices
- Advice to the Minister of Finance on insurance matters
- Compliance with Financial Transactions Reporting Act (FTRA) and Anti- Money Laundering (AML) legislation.

Corporate Governance - The Insurance Act, 2005, made provisions for the appointment of a maximum of seven commissioners, including The Superintendent of Insurance, the Deputy Superintendent of Insurance and three to five other members, comprised of persons with a wide experience in the areas of insurance, finance, commerce, law or administration; and are appointed by the Governor-General after consultation with the Minister of Finance. The Board of Commissioners meet at least once per month and are responsible for the overall governance of the Office of the Commission and for the establishment of related policies.

Management - The Insurance Act, 2005, made provisions for the appointment of a Superintendent and Deputy Superintendent of Insurance, with the responsibility of managing the day-to-day affairs of the Commission. They are both supported by a management team comprising of various professionals from the Insurance, finance, commerce, law, information technology and administration sectors.

The Commission's main offices are in the Silk Cotton House on Prospect Ridge Road, Nassau, New Providence, Bahamas. More information can be found on the Commission's website: www.icb.gov.bs.

1. Introduction

1.1 Purpose of this Guidance

This Framework supports **consistency and due diligence** in internal audit functions across all licensees of the Insurance Commission of The Bahamas ("The Commission"). It enhances assurance, enterprise risk management (ERM), supports regulatory compliance under the Insurance Act of 2005, and aids in safeguarding policyholder interests.

1.2 Applicability

Applies to domestic insurers, reinsurers, intermediaries, outsourced internal audit providers, and Audit Committees in The Bahamas.

1.3 Role of Internal Audit

Internal Auditing is a professional activity intended to help organizations achieve their stated objectives through both a systematic and strategic approach. Through their work, Internal Auditors implement annual audit plans, as well as perform advisory and support services which are often consistent with Internal Auditing Standards. Internal Auditors act as independent assurance providers, evaluating the adequacy of Governance, Risk Management, and Control Systems—essentially, complementing Management and External Audit functions.

2. Regulatory & Legal Context

Fundamentally, Internal Auditors must develop audit programs that comply with:

- **Insurance Act, 2005 (amended) -** The Insurance Act 2005, which came into force on July 1, 2009, introduced a new system for licensing and regulating domestic insurers based on the international standards prescribed by the Financial Action Task Force (FATF) and the core principles of the International Association of Insurance Supervisors (IAIS).
- **Insurance (General) Regulations –** Pursuant to powers conferred by section 233 of the Insurance Act 2005, the Insurance (General) Regulations serves as a supplemental statutory document which extends the Commission's regulatory framework and provides further guidance to its' licensees with respect to its operating, financial and compliance activities, as well as reporting requirements.
- **ICB Governance Guidelines -** Pursuant to section 234 of the Insurance Act 2005 (the Act), the Insurance Commission of The Bahamas **(**the Commission) issued guidelines to assist registrants and licensees under the Act to understand their

obligations for effective corporate governance. The purpose of this guidance note is to provide an overview of the characteristics, responsibilities, and key elements involved in good corporate governance which contribute to the entity's overall risk rating. The assessment criteria provide guidance to Senior Management, Board of Directors and other oversight functions. The Assessment Criteria is also used to guide supervisory judgment in assessing an insurer's risk profile.

- **AML/CFT Standards (ICB, Financial Intelligence Act 2000 and Central Bank Guidelines) –** Periodically updated to provide guidance to facilitate both public and private sector stakeholders (together, stakeholders) in identifying, assessing, understanding and mitigating their proliferation financing risks. The guidelines also aim to facilitate stakeholders in implementing their proliferation financing obligations.

  For further details, please log onto the ICB's website; www.icb.gov.bs and navigate to the 'legal' tab to download: www.icb.gov.bs/legal/legislation

Regulatory Expectations:

- Independence of the Internal Audit function – reporting directly to the Audit Committee/Board of Directors and in lieu of the Board being present based on the nature size and complexity of an organization, as is the case with many intermediaries, the Head of Internal Audit should report to the most senior executive position (e.g. CEO)
- Assurance on solvency, policyholder protections, and financial reporting.
- Governance support via evidence-based assurance.
- Control reviews on claims, underwriting, reinsurance, and Anti-money Laundering (AML)/Combating the Financing of Terrorism (CFT), Counter Proliferation Financing (CPF).

3. Internal Audit Mandate

All entities should maintain a formal Internal Audit Charter—with the following elements:

- **Purpose & Authority - Mission and Purpose –** The charter should define both the mission and the purpose of the internal audit function. The mission should be to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. Internal audit's independent and objective assurance and consulting services should be designed to add value and improve the organization's operations.
- **Adherence to the International Standards for the Professional Practice of Internal Auditing –** The charter should include details about how the internal audit function governs itself and how it adheres to the Institute of Internal Auditor's (IIA's) International Professional Practices Framework (IPPF), including:
    - Standards
    - Core principles for the professional practice of internal auditing
    - Definition of internal auditing
    - Code of ethics
- **Authority –** The charter should define the Chief Audit Executive's (CAE's) functional and administrative reporting relationship in the organization as noted above. In addition, a statement should be included affirming that the governing body will establish, maintain, and ensure that the Internal Audit function has sufficient authority to fulfill its duties.
- **Independence** —The Charter should state that the CAE will ensure independence and objectivity of the internal audit function to carry out its duties in an unbiased manner. If independence or objectivity is impaired, the CAE will disclose the details of the impairment to the Board of Directors and in the case where there is no Board, the CEO ("appropriate" parties). Furthermore, internal audit staff should have no direct operational responsibility or authority over any of the activities audited.
- **Scope** — this includes affiliates and outsourced functions. The charter should include a statement that the scope of the internal audit activities encompasses, but is not limited to, objective examinations of evidence for the purpose of providing independent assessments on the adequacy and effectiveness of governance, risk management, and control processes. Additionally, the charter should state that the CAE will report periodically to senior management and the governing body on the results of its department and the work the activity performs.

- **Responsibility** – The Charter should include statements regarding the responsibility for:
    - Submitting at least annually a risk-based internal audit plan.
    - Communicating with senior management and the governing body about the impact of resource limitations on the plan.
    - Ensuring the internal audit activity has access to appropriate resources regarding competency and skill.
    - Managing the activity appropriately for it to fulfill its mandate.
    - Ensuring conformance with IIA Standards
    - Communicating the results of its work and following up on agreed-to corrective actions.
    - Coordination with other assurance providers

Key Responsibilities:

1. Risk-based assurance across key processes
2. Governance and Enterprise Risk Management (ERM) reviews
3. Regulatory compliance oversight
4. Advisory input on new initiatives

- **Quality Assurance and Improvement** Program – The Charter should include:
    - A statement that the internal audit activity will maintain a quality assurance and improvement program that covers all aspects of the internal audit activity including its evaluation of conformance to IIA Standards.
    - A requirement for the CAE to report periodically the results of its quality assurance and improvement program to senior management and the governing body and to obtain an external assessment of the activity at least once every five years

4. ERM Integration

Following the “Three Lines” model/structure: this refers to the modernized, collaborative model, which emphasizes strategic alignment and communication across three (3) key functions:

1. The first line (**Operational Management**) owns and manages risks.
2. The second line (**Risk and Compliance Functions**) provide risk oversight and guidance and,
3. The third line (**Internal audit**) offers independent assurance.

Effective integration involves clear roles, comprehensive policies, continuous training, and a culture of collaboration between the lines to achieve organizational objectives through a cohesive risk management approach.

4.1 Governing Body/Board:

Provides strategic direction and ultimate oversight of the entire risk management framework, ensuring alignment with organizational goals.

- **1st Line**: Business accountability - **(Management):**

  The front-line business units and operational managers are responsible for identifying, assessing, and managing risks as part of their daily activities to achieve objectives.

- **2nd Line**: **Risk Management & Compliance Oversight:**

  Functions like risk management, compliance, legal, and finance that provide oversight, develop policies, and support the first line in managing risks effectively.

- **3rd Line**: **Internal Audit assurance**

  Internal auditors provide independent and objective assurance and advice on the effectiveness of the governance, risk management, and internal control processes.

  “Insurance-specific Risks” – The Board of Directors is responsible for the establishment and oversight of the ERM framework. It is vital that clear reporting lines are identified to ensure that the associated risks of decisions and/or processes are communicated timely to Management and the Board.

4.2 UNDERWRITING & SELECTION

The Internal Audit function must evaluate the **risk culture**, and link findings to ERM. Best practices with respect to the underwriting activities are as follows.

a) **Risk Identification** - Routinely identify all reasonably foreseeable and material underwriting risks, such as those from policyholder options. In doing so, consideration should be given to both internal and external sources and the interdependences between different risks.

b) **Risk Assessment and Measurement**: Quantify the identified risks by assessing their potential impact and probability of occurrence. Employ forward-looking techniques to evaluate these risks over a reasonable time horizon (e.g., at least three years).

c) **Risk Appetite**: Define and establish a clear risk appetite that guides decision-making and aligns with the insurer's corporate objectives and strategic planning.

d) **Risk Control and Mitigation:** Develop and implement policies and procedures to control risks and minimize their impact. Also, use risk management techniques like avoidance, mitigation, acceptance, and transference where appropriate.

e) **Risk Monitoring and Reporting:** Continuously monitor the results of risk identification and quantification activities. Additionally, establish robust reporting mechanisms to keep the board, risk committees, and senior management informed of risk exposures and the effectiveness of risk management actions.

f) **Integration with Business Operations:** Embed the ERM framework into the daily operations and strategic direction of the insurer. Link risk management activities to the management of capital adequacy and solvency.

4.3 CLAIMS LEAKAGE & FRAUD RISKS:

(I) Integrate into the ERM Framework

a) **Governance:**

A robust ERM framework requires board and senior management oversight, with clear accountabilities for managing claim and fraud risks.

b) **Strategy Alignment:**

Ensuring claims and leakage risk management aligns with the insurer's overall business goals and strategic objectives.

c) **Risk Appetite:**

Define acceptable levels of risk (risk appetite) for claim costs and leakage and establish policies that reflect these levels.

(II) Identify and Assess Risks

a) **Risk Identification:**

Proactively identify all potential sources of claim and leakage fraud, such as internal fraud, external fraud schemes, and inefficiencies in claims processing.

b) **Risk Assessment:**

Evaluate the likelihood and potential impact of identified risks. This includes quantitative analysis of financial exposure and qualitative assessments of reputational and operational impacts.

(III) Implement Risk Mitigation Strategies

a) **Process Redesign:**

Streamline claims handling processes to reduce manual errors, improve efficiency, and minimize opportunities for fraud.

b) **Technology and Analytics:**

Leverage advanced data analytics, machine learning, and AI to detect fraudulent patterns and predict high-risk claims, enabling faster and more accurate responses.

c) **Internal Controls:**

Develop and implement strong internal controls to prevent, detect, and respond to fraudulent activities.

d) **Staff Training:**

Train claims adjusters and other relevant staff to recognize red flags and follow established procedures for handling potential fraud.

(IV) Monitor and Report

a) **Key Risk Indicators (KRIs):**

Establish KPIs to monitor claim leakage and fraud metrics (e.g., claim cycle times, fraud detection rates, cost of claims).

b) **Regular Reporting:**

Implement a system for regular reporting on the performance of claim and fraud risk management activities to senior management and the board.

c) **Continuous Improvement:**

Use data and reporting to identify emerging risks and continuously refine risk management strategies and controls.

4.4 REINSURANCE EXPOSURE

Managing Reinsurance exposure risks within an Enterprise Risk Management (ERM) framework involves identifying, assessing, and controlling risks related to transferring liability to reinsurers, using tools like risk registers and risk assessment tools to monitor performance and exposure, and integrating Reinsurance with overall business strategy and capital needs. Key steps include thoroughly understanding the terms of Reinsurance contracts, continuously monitoring the cedent's own underwriting and risk exposures, and assessing the financial stability and performance of the Reinsurer to ensure they can meet their obligations.

1. Integration with ERM Framework

a) **Align with Strategy:**

Embed reinsurance risk management within the ERM framework, linking it to the insurer's strategic goals, business operations, and capital requirements.

b) **Holistic Risk Assessment:**

Understand how reinsurance decisions affect the insurer's overall risk profile and other identified risks, ensuring that risk exposures are viewed in relation to each other.

2. Identification and Assessment

a) **Identify Reinsurance Risks:**

Recognize potential issues, such as uncollectible Reinsurance (Reinsurance risk) or excessive concentration of risk with one Reinsurer.

b) **Risk-Based Approach:**

Tailor the risk management approach to the scale and complexity of the insurer's operations and its specific risk profile.

c) **Risk Registers:**

Use risk registers to document Reinsurance risks, their potential impact, and the actions being taken to manage them.

3. Control and Mitigation

a) **Thorough Due Diligence:**

Conduct due diligence on potential Reinsurers to assess their financial strength and ability to fulfill their obligations.

b) **Contractual Controls:**

Clearly define the terms and conditions of the Reinsurance contract to manage the cedent's exposure effectively.

c) **Monitoring Performance:**

Regularly monitor the performance and stability of Reinsurers and the effectiveness of the Reinsurance program in reducing the cedent's risk exposures.

4. Monitoring and Reporting

a) **Continuous Monitoring:**

Actively monitor both the cedent's risk exposures and the performance of the Reinsurance program to identify emerging issues.

b) **Reporting:**

Ensure clear and timely reporting of Reinsurance risks and the effectiveness of the mitigation strategies to the board of directors and other stakeholders.

5. Strategic Considerations

a) **Balance Risk Transfer and Retention:**

Determine the appropriate balance between transferring risk to Reinsurers and retaining it, aligning this decision with the insurer's overall risk appetite.

b) **Capital Management:**

Consider how Reinsurance affects capital requirements, ensuring that the strategy supports the insurer's capital adequacy and longer-term financial goals.

4.5 INVESTMENT VALUATION RISK

To manage investment valuation risks within an Enterprise Risk Management (ERM) framework for an insurance company, you must establish a comprehensive process including identifying valuation risks like market volatility and interest rate changes, assessing their likelihood and impact through metrics and modeling, mitigating them via diversification and hedging, monitoring them continuously, and reporting them to ensure regulatory compliance and strategic alignment with the

insurer's risk appetite. This integrated approach, led by strong governance, ensures these risks are managed holistically, protecting capital and supporting long-term business goals.

1. Risk Identification and Assessment

a) **Identify Valuation Risks**:

Pinpoint specific risks that could impact the value of the insurer's investments, such as market risk (equities, bonds), interest rate risk, credit risk (defaults), liquidity risk, and asset concentration risk.

b) **Assess Impact and Likelihood**:

Use quantitative methods like scenario analysis and sensitivity testing to gauge the potential financial impact of these risks and assign likelihood ratings to prioritize mitigation efforts.

2. Risk Mitigation and Control

a) **Implement Diversification**:

Spread investments across different asset classes, geographies, and sectors to reduce the impact of adverse performance with respect to any single investment class.

b) **Employ Hedging Strategies**:

Utilize financial instruments like derivatives to offset potential losses arising from market fluctuations, such as interest rate movements or equity price drops.

c) **Establish Limits and Triggers**:

Set clear investment limits for asset classes and exposure levels, along with early warning triggers for when these limits are approached, signaling a need for action.

3. Monitoring and Reporting

a) **Establish Key Risk Indicators (KRIs)**:

Develop metrics to track investment portfolio performance and risk exposure, allowing for ongoing monitoring against predefined risk appetite levels.

b) **Implement Regular Reporting**:

Provide regular, comprehensive reports on investment performance and risk to the board of directors and senior management to maintain oversight and ensure accountability.

c) **Use Technology**:

Leverage ERM digital platforms to host, summarize, and track risks, enabling more efficient monitoring and improved communication.

4. Governance and Strategy Alignment

a) **Define Risk Appetite**:

Clearly articulate the insurer's tolerance for investment valuation risks, ensuring it is aligned with the overall business strategy.

b) **Promote a Sound Risk Culture**:

Foster a company-wide culture where risk is discussed openly and all stakeholders understand their role in managing risks, starting from the board of directors.

c) **Ensure Integrated Framework**:

Treat investment valuation risk within the broader ERM context, understanding its interdependencies with other risk types like insurance and operational risks.

4.6 SOLVENCY/BALANCE SHEET WEAKNESS

ERM for solvency purposes is the coordination of risk management, strategic planning, capital adequacy, and financial efficiency to enhance sound operation of the insurer and ensure the adequate protection of policyholders.

1. *Review of actuarial reports and stress testing completed by Actuary (Life Insurers) to mitigate risks associated with performing and reliance on the actuarial function. Risks of Inaccurate Review of Actuarial Stress-Testing Reports in the Insurance Industry include:*

I. **Underestimation of Capital Requirements**

If stress scenarios, assumptions, or results are inaccurately reviewed, the insurer may significantly **underestimate capital needed** to withstand adverse events. This creates a risk of **falling below regulatory capital adequacy** thresholds, leading to supervisory intervention or operational restrictions.

II. **Incorrect Pricing, Reserving, or Product Strategy**

Stress testing feeds into pricing and reserve adequacy decisions. An inaccurate review can cause:

- Under-reserving for future claims
- Incorrect premium rate setting

- Misalignment of product profitability and risk tolerances

This can materially impair long-term solvency.

III. Regulatory Non-Compliance

Insurance regulators expect accurate, well-validated actuarial stress testing. Inaccurate review can lead to:

- Findings in regulatory inspections
- Fines or sanctions for misreporting
- Mandatory capital injections
- Increased supervisory scrutiny

This damages the company's reputation and consumes management resources.

IV. Inadequate Risk Appetite and Risk Management Decisions

Stress-testing results help management assess:

- Market risk
- Credit risk
- Catastrophe risk
- Underwriting and claims volatility
- Liquidity stress

If results are improperly reviewed or errors go undetected, the Board may make decisions based on **false risk exposures**, leading to strategic missteps or excessive risk-taking.

V. Overstated Financial Strength

A faulty review may inadvertently allow optimistic assumptions to pass unchallenged. This may result in:

- Overstated solvency ratios
- Misleading financial reporting

- Inaccurate ORSA (Own Risk and Solvency Assessment) outcomes

Stakeholders, including policyholders, investors, and regulators—may be misled about the company's true financial position.

VI. Failure to Identify Emerging or Extreme Risks

Actuarial stress tests often highlight new or evolving threats (e.g., climate risk, pandemic risk, cyber risk).
Inaccurate review can cause:

- Blind spots in risk identification
- Missed early warning signals
- Failure to update contingency plans

This leaves the insurer vulnerable to high-impact, low-probability events.

VII. Poor Investment and Asset-Liability Management (ALM) Decisions

Stress testing supports:

- Liquidity planning
- Asset mix strategy
- Duration matching
- Impact of market shocks

Errors or incomplete reviews can lead to:

- Liquidity shortages in stress events
- Mismatched assets and liabilities
- Losses from interest-rate or market volatility

VIII. Increased Probability of Insolvency

Cumulative failures in assessing capital, reserves, risks, and liquidity under stressed conditions create a **material risk of insolvency** during adverse periods.

IX. Reputational Damage

Significant misstatements or regulatory findings caused by inaccurate actuarial reviews undermine confidence from:

- Policyholders
- Brokers and agents
- Regulators
- External auditors
- Rating agencies

This can impact market competitiveness and business growth.

X. Internal Control Failure

Repeated inaccuracies suggest:

- Weak oversight
- Inadequate quality review procedures
- Poor actuarial governance
- Insufficient technical expertise

This creates broader operational risks and may warrant internal audit or regulatory intervention.

2. *(Section 2) Key Metrics recommended for the Internal Audit Function to Assess Insolvency Risk of General Insurers (including but not limited to):*

(i.) Capital Adequacy & Solvency Metrics

(a) Solvency Ratio / Capital Adequacy Ratio

- Measures Available Capital vs. Regulatory Required Capital.
- A primary early-warning indicator of financial stress.

(b) Minimum Capital Test (MCT) / Risk-Based Capital (RBC) Ratio

- Adjusts capital requirement based on underwriting, credit, market, and operational risks.
- Low RBC/MCT ratios indicate elevated insolvency risk.

(c) Margin of Solvency

- Surplus assets over liabilities.
- Assessed for sufficiency under base and stressed conditions.

(ii.) Claims & Reserving Adequacy Metrics

a) **Loss Ratio (Incurred Losses / Earned Premiums)**

- High or deteriorating loss ratios may indicate pricing or underwriting deficiencies.

b) **▪ Claims Development Triangles & Reserve Adequacy Tests**

- Used to identify reserve deficiencies or volatility in long-tail lines.

c) **▪ Claims Settlement Speed / Claims Outstanding Backlog**

- Slow settlement may indicate operational weaknesses or inadequate reserving.

d) **▪ Reserve Coverage Ratio**

- Reserves relative to expected future claims.
- Key indicator of potential reserve shortfalls.

(iii.) Underwriting Performance & Pricing Metrics

a) **Combined Ratio**

- Loss Ratio + Expense Ratio.
- A ratio over 100% suggests ongoing underwriting losses that can erode capital.

b) **▪ Underwriting Leverage Ratio (Net Written Premium / Capital & Surplus)**

- High leverage signals possible overextension and increased insolvency risk.

c) **▪ Premium Growth vs. Capital Growth**

a) Rapid premium growth without corresponding capital increases is a red flag.

(iv) Liquidity & Asset Quality Metrics

a) **Liquidity Ratio (Liquid Assets / Short-Term Liabilities)**

- Ensures claims and operating obligations can be met even under stress.

b) ▪ **Asset-Liability Matching (Duration Gap & Cash Flow Testing)**

- Misalignment may lead to liquidity shortages during market stress.

c) ▪ **Investment Concentration / Asset Diversification Metrics**

- Overexposure to a single asset class or issuer increases risk.

d) ▪ **Credit Quality of Investments**

- Regulators assess the share of assets rated below investment grade.

(v) Reinsurance Structure & Risk Transfer Metrics

a) Reinsurance Dependence Ratio

- Heavy reliance may expose the insurer to counterparty risk.

b) Reinsurance Recoverable Balances / Capital Ratio

- Large recoverable or receivables may be uncollectible under stress situations.

c) Reinsurer Credit Quality

- Regulators monitor AM Best or equivalent ratings to assess counterparty solvency.

d) Net Retention Ratio

- Indicates exposure retained after cessions; too low or too high can signal concern.

(vi) Operational & Governance Risk Metrics

a) Compliance with Internal Controls & Risk Management Standards

- Weak governance is an indicator of future solvency issues.

b) Frequency and Severity of Audit Findings

- Persistent unresolved deficiencies elevate insolvency risk.

c) Actuarial Review Quality Indicators

- Quality and independence of appointed actuary reports.
- Adequacy of stress testing and scenario analysis.

(vii) Profitability & Sustainability Indicators

a) ROE (Return on Equity) & ROA (Return on Assets)

- Negative or highly volatile returns can impair capital over time.

b) Expense Ratio (Operating Expenses / Earned Premium)

- Inefficiency or cost inflation can worsen underwriting results.

c) Multi-year Performance Trends

- Regulators examine 3–5 years of metrics for sustainability.

(viii) Catastrophe & Concentration Risk Metrics

a) ▪ Probable Maximum Loss (PML) vs. Capital

- Particularly relevant for hurricanes, earthquakes, and regional hazards.

b) ▪ Catastrophe Reinsurance Adequacy

- Assessing layering, limits, reinstatement protection, and exhaustion points.

c) ▪ Geographic or Line-of-Business Concentration

- High exposure concentration increases insolvency susceptibility.

(ix) Stress Testing & Scenario Analysis Metrics

a) Regulators evaluate the insurer's ability to withstand:

- Catastrophic events
- Economic downturns
- Large single-event claims
- Adverse reserve development
- Market volatility

b) Metrics include solvency ratio post-stress, liquidity under stress, and capital erosion.

(x.) Market Conduct & Policyholder Behavior Indicators

a) Although less direct, market conduct issues can create financial liabilities:

- Unfair claims practices
- Mis-selling
- High lapse or cancellation rates

Regulators see these as **leading indicators of potential insolvency** and hence Internal Audit functions should incorporate a thorough review of policies and procedures in addition to test of internal controls incorporated within their Annual Audit Plans for General Insurance operations.

4.7 CYBER/DATA RISK

To manage cyber and data risks within an insurance ERM framework, an insurer should establish strong governance, implement comprehensive technical controls like encryption and multi-factor authentication, conduct regular risk assessments using frameworks such as NIST[1], and prioritize employee training on cyber threats. Central to this process is a continuous cycle of identification, assessment, mitigation, and monitoring, alongside a formal third-party risk management program, to protect sensitive client data and maintain operational resilience against evolving threats.

1. Establish Governance and Infrastructure

a) **Formal Cybersecurity Governance:**

Implement a formal, established cybersecurity governance structure and cyber risk management framework to guide policies and procedures.

b) **Dedicated Team:**

Ensure there is a dedicated team or function responsible for IT compliance and cybersecurity risk.

2. Conduct Risk Identification and Assessment

a) **Regular Assessments:**

[1] The NIST Cybersecurity Framework (CSF) is a voluntary set of guidelines and best practices from the National Institute of Standards and Technology (NIST) designed to help organizations better manage and reduce their cybersecurity risks. It provides a structured approach with five core functions—Govern, Identify, Protect, Detect, Respond, and Recover—to help organizations implement and improve their cybersecurity risk management programs. The CSF is adaptable and helps organizations communicate about cybersecurity risks internally and externally, align cybersecurity efforts with business goals, and make risk-informed decisions about resource allocation.

Perform consistent and systematic cyber risk assessments to identify vulnerabilities and potential impacts.

b) **Utilize Frameworks:**

Adopt established frameworks like the NIST Cybersecurity Framework to provide a structured approach to risk assessment and management.

c) **AI-Powered Tools:**

Leverage AI and machine learning to analyze trends, predict risks, and identify high-risk areas for deeper investigation.

d) **Third-Party Risk Management:**

Develop a structured process to assess and manage risks associated with third-party vendors and partners in the supply chain.

3. Implement Robust Mitigation Strategies

a) **Technical Controls:**

Deploy security measures such as firewalls, encryption, multi-factor authentication, and regular data backups to protect sensitive data and systems.

b) **Security & Fraud Detection Software:**

Implement automated tools for cyber threat detection and fraud prevention.

c) **Employee Training:**

Regularly train employees on cyber threats, data privacy, and secure data handling practices to mitigate human-related vulnerabilities.

d) **Incident Response Plan:**

Develop and regularly test a comprehensive incident response plan to effectively manage and recover from cyber incidents.

4. Monitor and Report

a) **Real-Time Dashboards:**

Utilize real-time risk dashboards to provide executives with a consolidated view of the organization's risk exposure.

b) **Formal Reporting:**

Ensure regular reporting on IT risks, cyber threats, and the effectiveness of mitigation strategies to the board and audit committee.

c) **Threat Intelligence:**

Establish methods to collect, analyze, and act on cyber threat intelligence to stay ahead of emerging threats.

5. Maintain Business Continuity

- **Business Continuity & Disaster Recovery:**

Ensure that the ERM framework incorporates robust business continuity and disaster recovery plans to maintain operations during and after a cyber incident.

- **Cyber Insurance:**

Secure adequate cyber insurance to provide a financial safety net and cover costs associated with a data breach or cyberattack.

- For more information, please refer to the Cybersecurity Guidelines issued by the ICB via our website. www.icb.gov.bs or via direct link: www.

4.8 OPERATIONAL & OUTSOURCING EXPOSURES

To manage outsourcing and operational risks within an ERM framework for an insurance company, the organization should integrate outsourcing risk management into its ERM processes, covering identification, assessment, response, and continuous monitoring of these risks across the company's strategic, operational, financial, and compliance areas. Key strategies include developing comprehensive outsourcing policies, conducting due diligence on vendors, establishing clear service level agreements, implementing strong contractual terms, and performing ongoing monitoring and auditing of third-party service providers to ensure they align with the insurer's overall risk appetite and strategic objectives.

Integrating Outsourcing Risk into the ERM Framework

1. **Governance and Culture:**
    a. **Leadership Commitment:** Establish a strong risk culture led by the board and senior management, emphasizing the importance of effective risk management in all outsourcing decisions.
    b. **Policies and Procedures:** Develop specific policies for outsourcing that align with the overall ERM framework, detailing acceptable outsourcing activities, risk tolerance, and required control measures.
2. **Risk Identification:**

a. **Comprehensive Risk Assessment:** Identify potential risks related to outsourcing, such as data breaches, business continuity failures, service quality issues, vendor insolvency, and non-compliance with regulations.

b. **Risk Register:** Document all identified outsourcing and operational risks in the enterprise risk register.

3. **Risk Assessment and Prioritization:**

- **Analyze Interdependencies:** Assess how outsourced functions affect other business units and the overall operational risk profile of the insurer.
- **Quantify Impact:** Evaluate the potential financial, reputational, and operational impact and likelihood of these risks to prioritize mitigation efforts.

4. **Risk Response and Mitigation:**

a. **Due Diligence:** Conduct thorough due diligence on potential vendors to assess their financial stability, security protocols, and operational capabilities.

b. **Contractual Safeguards:** Implement strong contractual clauses in outsourcing agreements that include performance standards, security measures, data privacy requirements, and business continuity plans.

c. **Vendor Management:** Establish a robust third-party management framework to oversee vendor performance and compliance.

d. **Contingency Planning:** Develop contingency plans for critical outsourced functions in case of vendor failure.

5. **Risk Monitoring and Reporting:**

a. **Key Risk Indicators (KRIs):** Implement KRIs to continuously monitor vendor performance and emerging risks.

b. **Audits and Reviews:** Conduct regular internal and external audits of outsourced activities to ensure compliance and effectiveness of controls.

c. **Regular Reporting:** Establish clear reporting channels to communicate outsourcing risks and performance to senior management and the board.

Other Key Considerations for Insurance Companies

d) **Regulatory Compliance:**

Ensure that the outsourcing and risk management framework complies with relevant Insurance regulations as outlined in both the Insurance Act 2005 and the Insurance (General) Regulations 2009.

4.9 Capital Adequacy:

Link outsourcing risk management to the management of capital adequacy and solvency, as required by The Insurance Act 2006. Take note of Minimum Capital Requirements (MCR), thereby aligning Board approved investment programs (including risk-appetite) with the statutory mandated MCR.

1. **Policyholder Protection:**

Maintain a focus on protecting policyholders' interests by ensuring that outsourced functions do not compromise the security and quality of services of all policyholders.

5. Internal Control Framework

Audits should evaluate controls across (but not limited to):

- **Underwriting** – price discipline, policy documentation
- **Claims** – segregation, fraud protocols
- **Reinsurance** – treaty terms, receipt controls
- **Investments** – compliance, valuation oversight
- **Financial Reporting** – policy and statutory requirements
- **AML/CFT** – KYC, suspicious activity monitoring

6. Risk-Based Audit Planning

Annual plans should follow:

1. Understand strategy, risk appetites
2. Consult management, risk, compliance
3. Catalogue inherent and residual risks
4. Prioritize by risk significance (financial, reputational, compliance, strategic)
5. Include emerging risks: Climate, Digital/Innovation initiatives, IFRS 17, Artificial intelligence, etc.

Plan requires Audit Committee approval and must be adaptable during the year.

7. Audit Methodology & Standards

All audits align with IIA Standards and ICB guidelines:

1. **Planning** – objectives, scope, methodology
2. **Fieldwork** – control testing, sampling
3. **Reporting** – findings, cause, rating
4. **Follow-up** – validation of action completion

Data Analytics should be used where feasible to test entire populations (large population of data such as all claims for the year in an Insurer).

8. Reporting & Communication

Key stakeholders:

- Audit Committee/Board
- Senior Management
- Regulators (ICB) if material findings are the result of internal audit and could impair the Insurers' capital and ability to settle claims or other obligations (reinsurance, commissions, etc.)

A well-structured report enhances clarity, credibility, and actionability. The Executive Summary (For Boards & Audit Committees) should be concise and convey the salient points and list material findings. It outlines the key risks and Internal Audit's approach and methodologies used.

Additionally, reports should include risk ratings, root cause analysis, and tracked action logs. See further guidance below:

b) Key Components of an Internal Audit Report:

1. **Title Page**
    - Report title
    - Audit area
    - Date of issuance
    - Prepared by (Internal Audit Department)
2. **Executive Summary**

- Brief overview of the audit objectives, scope, and key findings.
- High-level recommendations.
- Overall audit opinion (if applicable).

3. **Background**
   - Description of the audited process, department or system.
   - Context for why the audit was performed.
4. **Objectives and Scope**
   - What the audit aimed to assess.
   - Time period covered.
   - Locations, systems, or processes reviewed.
5. **Methodology**
   - Audit techniques used (e.g., interviews, sampling, walkthroughs).
   - Standards followed (e.g., IIA, ISO).
6. **Findings**
   - Clearly numbered and categorized (e.g., High, Medium, Low risk).
   - Each finding should include:
     - **Condition**: What was observed.
     - **Criteria**: What should happen (policy, regulation, best practice).
     - **Cause**: Why the issue occurred.
     - **Effect**: Impact or risk posed.
     - **Recommendation**: Action to address the issue.
     - **Management Response**: Agreed action and timeline.
7. **Conclusion / Audit Opinion**
   - Summary of overall control effectiveness.
   - May include a formal rating (e.g., satisfactory, needs improvement).
8. **Appendices**
   - Supporting data, charts, process maps, or detailed observations.

- Audit team members and contact info.

9. Challenges & Considerations

- **Scale & outsourcing** by smaller insurers
- **Regulatory updates** require responsive audit plans
- **Reinsurance complexity** – foreign counterparties
- **Digital transformation** and cyber risk need stronger IT focus

10. Best Practices

- Uphold **independence and objectivity**
- Conduct **thematic and deep-dive audits** on AML/CFT, fraud
- Build an **audit skills matrix** for specific competencies
- Co-operate with risk and compliance lines, while ensuring assurance independence
- Stay current with **Solvency II**, IFRS 17, global risk frameworks

11. Competence & Ethics

- Comply with the **IIA Code of Ethics**
- Recommended accreditations: CIA, CISA, CPCU
- Ongoing training in insurance regulation, AML/CFT, and data analytics is essential

12. Sample Tools

1) Internal Audit Charter (Insurance Company)

The Internal Audit Charter is a foundational document that defines the purpose, authority, and responsibility of the internal audit function within an organization. Its importance lies in both governance and operational clarity. Here's a breakdown of why it's essential:

a) Establishes the Purpose of Internal Audit

- Clarifies the role of internal audit in evaluating risk management, control, and governance processes.

- Aligns the audit function with the organization's strategic objectives.

b) 2. Grants Authority

- Empowers internal auditors to access records, personnel, and physical properties relevant to audits.
- Ensures independence from operational management, which is critical for objectivity.

c) 3. Defines Scope and Responsibilities

- Outlines what internal audit will and won't do (e.g., assurance vs. consulting).
- Specifies responsibilities such as:
    - Risk assessments
    - Compliance reviews
    - Operational audits
    - Reporting to the Audit Committee or Board

d) 4. Supports Independence and Objectivity

- Reinforces that internal audit reports functionally to the Board or Audit Committee, not management.
- Helps prevent conflicts of interest and undue influence.

e) 5. Enhances Accountability and Transparency

- Provides a clear framework for evaluating the performance of the internal audit function.
- Ensure stakeholders understand the value and limitations of internal audit.

f) 6. Aligns with Professional Standards

- Required by the International Standards for the Professional Practice of Internal Auditing (IPPF) issued by the Institute of Internal Auditors (IIA).
- Helps ensure compliance with global best practices.

In addition to the Chief Audit Executive's signature, the Internal Audit Charter must be signed by the Chair of the Audit Committee and ideally the Chairman of the Board.

g) e.g. **Sample Internal Audit Charter - Insurance Company – Internal Audit Unit**

1. Purpose

The purpose of the Internal Audit Charter is to formally define the mandate, authority, responsibilities, and accountability of the Internal Audit Unit ("IAU") of the Company. The IAU exists to provide independent, objective assurance and advisory services designed to add value and improve the Company's operations, governance, and risk management framework.

The Unit assists the Board of Directors and Executive Management in accomplishing strategic, operational, financial, and compliance objectives by evaluating the adequacy and effectiveness of internal controls and recommending improvements.

2. Authority

The Internal Audit Unit is authorized to:

1. **Full and unrestricted access** to all functions, information systems, records, physical properties, and personnel relevant to audit engagements.
2. **Direct and unrestricted communication** with the Board of Directors, the Audit Committee, Managing Director/CEO, and Senior Executives.
3. **Allocate resources**, determine audit scope, select audit techniques, and apply professional judgment in performing work.
4. **Obtain necessary assistance** of personnel within the Company and access external subject matter experts when required.

The Internal Audit Unit is **not authorized to** perform operational duties, initiate or approve transactions, or direct activities of employees outside the IAU, except in the context of audits.

3. Independence and Objectivity

To maintain independence and objectivity:

- The internal auditor(s) report functionally to the **Audit Committee of the Board** and administratively to the **Managing Director/CEO**.
- The IAU shall have no direct responsibility for developing or implementing internal controls, operational procedures, or decision-making processes.
- Internal auditors must avoid any conflicts of interest and shall adhere to the International Standards for the Professional Practice of Internal Auditing (IIA Standards) and the Code of Ethics issued by The Institute of Internal Auditors.

4. Scope of Work

The Internal Audit Unit's scope includes, but is not limited to:

1. **Evaluating the adequacy and effectiveness** of risk management, internal controls, governance, and compliance systems.
2. **Reviewing operational efficiency** and resource utilization across all departments, including Underwriting, Claims, Finance, Reinsurance, Human Resources, IT, and Compliance.
3. **Assessing financial and regulatory reporting** processes to ensure accuracy, integrity, and compliance with applicable insurance laws and statutes.

4. **Evaluating safeguarding of assets**, including IT systems, customer data, and sensitive financial information.
5. **Reviewing adherence to policies**, procedures, and legal/regulatory requirements from the Insurance Commission and other authorities.
6. **Conducting special investigations** related to fraud, misconduct, or other irregularities, as required.
7. **Following up on audit recommendations** to ensure corrective actions are implemented.

5. Responsibilities

The Internal Audit Unit shall:

- Develop a **risk-based annual audit plan** for approval by the Audit Committee.
- Execute audits in accordance with IIA Standards.
- Report significant findings, control weaknesses, and recommendations to Management and the Audit Committee.
- Provide **quarterly reports** to the Audit Committee summarizing audit activities, emerging risks, and progress of remediation efforts.
- Maintain a high level of professional competence through continuous training.
- Coordinate with external auditors and regulators to promote efficient coverage and reduce duplications.

6. Reporting

The Internal Auditor shall:

- Issue written audit reports to Senior Management and the Audit Committee after each engagement.
- Include the purpose, scope, methodology, findings, root cause analysis, risk implications, and recommended corrective actions.
- Report serious or material control breaches immediately to the Audit Committee Chairperson and Managing Director/CEO.
- Provide an annual assessment on the overall adequacy and effectiveness of internal controls.

7. Accountability

The Internal Audit Unit is accountable to the Audit Committee for:

- Proper execution of the approved audit plan.
- Quality and professionalism of audit work.
- Reporting significant risk exposures and control issues.
- Maintaining independence and objectivity.

- Ensuring that audit recommendations are monitored and resolved.

8. Standards of Practice

The Internal Audit Unit shall conduct its activities in accordance with:

- The **International Standards for the Professional Practice of Internal Auditing**
- The **Code of Ethics** of The Institute of Internal Auditors
- Applicable insurance legislation and regulatory requirements
- Internal policies and governance guidelines of the Company

9. Review of Charter

This Internal Audit Charter shall be reviewed **annually** or as required to ensure relevance and alignment with professional standards, regulatory requirements, and changes in the Company's operating environment. Any amendments must be approved by the Audit Committee.

10. Approval

This Internal Audit Charter is approved by the Audit Committee of the Board of Directors and becomes effective on the date indicated below.

_____
Chairperson, Audit Committee

_____
Date:

2) Risk-Based Audit Plan Outline

QUARTER	AUDIT AREA	RISK CATEGORY	SCOPE HIGHLIGHTS
Q1	Underwriting & Product Pricing	Underwriting Risk	Pricing models, policy document controls
Q2	Claims Management	Claims & Operational	Segregation, fraud, leakage
Q3	Reinsurance Review	Counterparty Risk	Treaty design, recoverable testing
Q4	AML/CFT Review	Compliance Risk	KYC, suspicious activity monitoring

3) Audit Issue Rating Matrix

Rating	***Description***	***Target Remediation Time***
High	Major failure, systemic, severe impact	1–2 months
Medium	Control weakness, moderate impact	3–4 months
Low	Minor issue, procedural or documentation-based	6–9 months

13. Key Regulatory References & Contacts

- **Insurance Act, 2005 (as amended)**: governance, solvency, reporting
- **General Insurance Regulations**
- **AML/CFT Guidelines** – ICB & Central Bank
- **Insurance Commission of The Bahamas**
  - Address: Silk Cotton House, Prospect Ridge, Nassau, Bahamas
  - Tel: +1 (242) 603-4183
  - Website: www.icb.gov.bs

14. Other Resources

a) Top 5 Sector-Wide Risks

1. **Underwriting & Pricing** – risk of non-competitive or underpriced products
2. **Claims Leakage & Fraud**
3. **Reinsurance Exposure** – relying on foreign counterparty performance
4. **Regulatory/Solvency Compliance** – capital adequacy and financial reporting
5. **Cybersecurity Risk** – data breach protection

b) Regulatory Requirements

- Insurance Act 2005, mandates internal governance and audit roles
- ICB expects assurance over solvency, financial reporting, and policyholder fund protection
- AML/CFT compliance is mandatory (ICB + Central Bank)

c) Internal Audit Role

- Provide **independent assurance** on internal controls and compliance
- Evaluate **ERM integration** and risk culture
- Report findings to the **Audit Committee** and senior management
- Track remediation of control deficiencies

d) Best Practices for Governance

- Approving a **risk-based annual audit plan** aligned to strategic objectives
- Ensure the Internal Audit Charter mandates **independence and scope authority**
- Utilize **subject matter experts** in understaffed areas (e.g. fraud, IT, AML)
- Require Audit Committee oversight and prompt remediation of high-priority issues

e) The Institute of Internal Audits has issued updated Standards (January 2025) that guide internal auditors in the execution of the Internal Audit Function. These standards are effective and internationally accepted in the profession of Internal Audit and should be referenced when conducting audits of licensees. The Commission references applicable internal audit standards below (for detailed

information on these and other professional standards issued by the institute of Internal Auditors, please visit the IIA's website: www.iia.org):

1. Standard 2000 – Managing the Internal Audit Activity

Covers planning, communication, and supervision of audit activities at the department level.

2. Standard 2100 – Nature of Work

Defines what internal audits should cover (risk management, control, governance).

Standards directly governing the audit engagement process (2200–2600):

3. Standard 2200 – Engagement Planning

Requires auditors to develop and document an audit plan for each engagement.

Related Standards:

- **2201 – Planning Considerations**
  Understanding the objectives, risks, controls, and processes.
- **2202 – Engagement Objectives**
- **2203 – Engagement Scope**
- **2204 – Engagement Resource Allocation**
- **2205 – Work Program**
  Specifies designing audit procedures.

4. Standard 2300 – Performing the Engagement

Outlines the execution of audit fieldwork.

Related Standards:

- **2310 – Identifying Information**
- **2320 – Analysis and Evaluation**
- **2330 – Documenting Information**
- **2340 – Engagement Supervision**
  These standards describe **how auditors gather evidence, analyze information, and document results.**

5. Standard 2400 – Communicating Results

Specifies how audit findings must be reported.

Related Standards:

- **2410 – Criteria for Communicating**
- **2420 – Quality of Communications**
- **2430 – Engagement Disclosure of Nonconformance**
- **2440 – Disseminating Results**

- **2450 – Overall Opinions**

6. Standard 2500 – Monitoring Progress

Governance of follow-up activities to ensure management implements corrective actions.

7. Standard 2600 – Communicating the Acceptance of Risks

Covers escalation when management accepts a level of risk that may be unacceptable.

Summary

The **core IIA standards** that explain *how to conduct an audit from planning to reporting* are:

2200 – 2600 Series

- **2200 – Engagement Planning**
- **2300 – Performing the Engagement**
- **2400 – Communicating Results**
- **2500 – Monitoring Progress**
- **2600 – Communicating the Acceptance of Risks**

These standards define the full **audit lifecycle**:
Plan → Execute → Report → Follow-up → Escalate (if needed).

IIA Standard that Relates to Peer Review

Standard 1312 – External Assessments

This is the IIA standard that corresponds directly to what is commonly called a **peer review**.

What it requires:

- Internal audit activities must undergo an **external quality assessment** at least **once every five years**.
- The assessment must be performed by a **qualified, independent assessor or assessment team** from outside the organization.
- A peer review can be done through:
  - A **full external assessment**, or
  - A **self-assessment with independent external validation (SAIV)**.

Key Points:

- External assessments determine the internal audit activity's **conformance with the IIA Standards**.
- Peer reviewers must be **competent, independent, and objective**.
- Results must be reported to **senior management and the board**.

f) Risk Heat Map (Example)

Risk Area	Likelihood	Impact	Overall Risk
Underwriting & Pricing	■■■	■■■	High
Claims Management	■■■	■■	High
Reinsurance	■■	■■■	Moderate
AML/CFT Compliance	■■	■■■	Moderate
Cybersecurity	■■■	■■	High

g) Board Action Points

- **Endorse** the Internal Audit annual plan
- **Ensure adequate resourcing** for internal audit expertise
- **Monitor remediation** of high-risk findings
- **Supporting ongoing professional development**

h) Conclusion

Internal Audit is a key pillar in maintaining **sound insurance industry governance**, **supporting solvency compliance**, **protecting policyholders**, and **enhancing market integrity**. Additionally, it plays a critical role in promoting transparency, accountability, and organizational resilience. Its importance extends beyond compliance, serving as a key driver of strategic improvement across all areas of operations:

1. **Risk Management:**
   Internal Audit provides independent assurance that risks—financial, operational, technological, and strategic—are properly identified, assessed, and mitigated. By evaluating the effectiveness of risk responses and controls, it helps management make informed decisions and maintain a proactive risk culture.

2. **Enhancing Operational Efficiency:**
   Through process reviews and advisory engagements, Internal Audit identifies inefficiencies and redundancies, recommending practical solutions to streamline workflows, optimize resources, and improve overall performance.

3. **Assessing the Effectiveness of Internal Controls:** Internal Audit evaluates whether internal controls are adequately designed, implemented, and functioning as intended. This continuous assessment strengthens the control environment, reduces exposure to errors or fraud, and supports accurate and reliable financial reporting.

4. **Strengthening Governance and Compliance:** By promoting adherence to laws, regulations, and internal policies, Internal Audit supports strong governance practices. It provides assurance to boards and senior leadership that ethical standards and regulatory requirements are upheld, thereby enhancing institutional integrity and stakeholder confidence. Board support and clear communication with Audit Committees are critical for its effectiveness.

The Insurance Commission of the Bahamas remains resolute on chartering a progressive and inclusive path toward the growth and sustained development of the Insurance sector in the Bahamas. The Internal Audit Guidelines issued within this document have taken into consideration international standards and best practices which have proven to be effective and applicable to the Insurance industry. For more information on the Commission and its guidelines or statutes, please log onto our website, www.icb.gov.bs or contact us at info@icb.gov.bs.

1. **Forms (required to be completed annually or periodically as required)**

- Fraud Reporting (Internal, policyholder, etc.)
- Statutory Breach – Self-reporting
- Statutory Compliance and Scope Limitation
- Exit Interview (Risk & Compliance Senior Executives) – Key Management (MLRO, Chief Audit Executive, Risk Officer)

The Insurance Commission of The Bahamas (ICB) requires Internal Audit Executives to submit the declarations (forms listed above) annually within 120 after the calendar year-ending December 31st).

INSURANCE COMMISSION OF THE BAHAMAS

Insurance Commission of The Bahamas – Compliance & Notification of Limitation of Scope Certification (Internal Audit)

[Name of Institution],

_____ Licensee Number: _____

Head of Internal Audit's Annual Certification to the Insurance Commission of The Bahamas

[This certification, required annually, within 120 days of the end of each calendar year, shall contain the following:]

a. I, _____, Head of Internal Audit of _____ confirm that the Insurance Commission of The Bahamas will be immediately notified of any scope limitations requested or imposed by the Licensee, or any obstacles to, or difficulties in obtaining information necessary to perform an audit.

b. I,_____, Head of Internal Audit of _____, confirm that any relevant material internal audit findings, particularly in the areas of AML/KYC controls, will be communicated to the Insurance Commission of the Bahamas without delay (prior to the mandated 120 period post calendar year-end, wherever applicable).

c. I, _____, Head of Internal Audit of_____, confirm internal audit's satisfaction with the licensee's compliance and its financial and regulatory reporting.

Submitted to:

Insurance Supervision and Market Conduct Unit – Insurance Commission of the Bahamas

_____ _____

Chief Audit Executive Date