



INSURANCE COMMISSION
OF THE BAHAMAS

GUIDELINES ON OUTSOURCING AND THIRD-PARTY RISK MANAGEMENT

SEPTEMBER 2026



INSURANCE COMMISSION
OF THE BAHAMAS



This consultative paper is issued by the Insurance Commission of The Bahamas for the purpose of public consultation. It remains the property of the Insurance Commission of The Bahamas. Any reproduction, distribution, or use of this document, whether in whole or in part, is prohibited without the express written permission of the Insurance Commission of The Bahamas. The views expressed in this paper are for consultation purposes only and do not represent a final position or policy decision of The Insurance Commission of The Bahamas.



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

Contents

- 1. Introduction and legal basis
- 2. Purpose and regulatory outcomes
- 3. Scope and application
- 4. Definitions
- 5. Proportionality and classification
- 6. Governance and accountability
- 7. Outsourcing policy and lifecycle framework
- 8. Pre-outsourcing risk assessment
- 9. Due diligence
- 10. Contractual and service-level requirements
- 11. Data, cybersecurity, cloud and cross-border arrangements
- 12. Sub-outsourcing
- 13. Ongoing monitoring and assurance
- 14. Business continuity, operational resilience and exit
- 15. Intra-group arrangements
- 16. Outsourced control functions
- 17. Notifications, approvals and incident reporting
- 18. Register and record keeping
- 19. Commission access and supervisory powers
- 20. Transition and consequences of non-compliance
- Appendix 1 – Materiality and criticality assessment
- Appendix 2 – Outsourcing register
- Appendix 3 – Notification/application form
- Appendix 4 – Minimum contractual clauses checklist
- Appendix 5 – Service level agreement schedule
- Appendix 6 – Annual Board attestation
- Appendix 7 – Benchmark adoption matrix

1. Introduction and legal basis

- 1.1. The Insurance Commission of The Bahamas (the “Commission”) issues these Guidelines to promote sound governance, prudent risk management, operational resilience and policyholder protection where a registrant or licensee relies on an external or intra-group service provider.
- 1.2. These Guidelines are issued pursuant to section 234 of the Insurance Act, Ch. 347, and the applicable guideline-making powers under the External Insurance Act, Ch. 348, as amended or replaced. They supplement, and do not replace, the Acts, regulations, licence conditions, directives, notices and other guidelines issued by the Commission.
- 1.3. These Guidelines must be read with the Commission’s Guidelines on Corporate Governance and Oversight Assessment Criteria, Guidelines for the Compliance Function, Guidance Framework for the Internal Audit Function, Guidance on Cybersecurity Risk Management, AML/CFT/CPF Guidelines, Guidelines for Assessing General Fitness and Propriety, and any applicable risk-based supervision framework.
- 1.4. Outsourcing does not transfer or reduce the statutory, fiduciary or regulatory obligations of a registrant or licensee, its Board, senior management, responsible officer or control functions. The regulated entity remains fully accountable for every outsourced activity and for the acts and omissions of its service providers in relation to that activity.
- 1.5. An arrangement must not impair the Commission’s ability to supervise the regulated entity, obstruct access to information, diminish policyholder protection, create undue operational dependency, or result in a shell or letter-box entity lacking adequate substance, expertise, decision-making capacity or records.

2. Purpose and regulatory outcomes

- 2.1. The purpose of these Guidelines is to establish minimum expectations across the entire outsourcing and third-party lifecycle.
- 2.2. A registrant or licensee should be able to demonstrate the following outcomes:
 - clear Board and senior-management accountability;
 - risk-based identification of material and critical arrangements;
 - proportionate due diligence, contracting, monitoring and assurance;
 - security, confidentiality, availability and recoverability of information and services;
 - continuity of important business services within approved impact tolerances;
 - orderly exit without unreasonable cost, disruption or regulatory breach; and
 - timely regulatory notification and unrestricted supervisory access.

3. Scope and application

- 3.1. These Guidelines apply to all registrants and licensees under the Insurance Act and External Insurance Act, including insurers, reinsurers, external insurers, insurance managers and intermediaries, subject to proportionality.
- 3.2. They apply to arrangements with related and unrelated parties, domestic and overseas providers, cloud and technology providers, and all material sub-outsourcing chains.

- 3.3.** A third-party arrangement that is not outsourcing must nevertheless be risk-managed where it may materially affect policyholders, regulated operations, data, compliance or the Commission's supervisory access.
- 3.4.** The following are ordinarily not outsourcing: purchase of standard utilities or goods; external legal opinions and one-off specialist advice; market information services; routine travel, catering, cleaning and premises maintenance; and services that do not form part of, support or materially affect a regulated activity. This exclusion does not remove obligations under the Cybersecurity Risk Management Guidance, data protection law or general risk-management duties.

4. Definitions

Term	Meaning
Board	the governing body of the registrant or licensee.
Critical arrangement	a material arrangement whose disruption could threaten viability, policyholder protection, an important business service, compliance with a statutory obligation, or the ability to meet an impact tolerance.
Important business service	a service delivered to policyholders or the market which, if disrupted, could cause intolerable harm to policyholders, market confidence or financial stability.
Material outsourcing	outsourcing whose failure or inadequate performance could materially impair financial condition, reputation, operations, governance, compliance, policyholder outcomes or supervisory access.
Outsourcing	an arrangement under which a service provider performs on a continuing or recurring basis a process, service or activity that would otherwise be undertaken by the regulated entity.
Service provider	a related or unrelated person that performs an outsourced or other relevant third-party service.
Sub-outsourcing	a service provider's transfer of a material element of the outsourced service to another provider.
Third-party arrangement	any business arrangement involving reliance on an external or intra-group person, whether or not it is outsourcing.

5. Proportionality and classification

- 5.1.** Requirements must be applied having regard to the nature, size, complexity and risk profile of the entity and the materiality and criticality of the arrangement. Proportionality changes the intensity of controls, however, it does not disapply the core outcomes in paragraph 2.2.
- 5.2.** Each arrangement must be classified before commitment and reviewed at least annually and upon material change as: (a) critical; (b) material but not critical; or (c) non-material.
- 5.3.** Control functions, core policy administration, underwriting decision-making, claims handling or settlement, actuarial services, custody or management of material assets, material cloud hosting, customer-data processing, cybersecurity monitoring, and systems supporting important business services will ordinarily be material. The Commission may determine that any arrangement is material or critical.
- 5.4.** Smaller entities and intermediaries may adopt simplified documentation and monitoring for non-material arrangements, but must retain written accountability, appropriate due diligence, confidentiality and security safeguards, incident escalation, termination rights and supervisory access.

5.5. Without limiting qualitative judgment, an arrangement is presumed material where any of the following applies: annual payments exceed the lesser of B\$1 million, 5 per cent of the entity's regulatory capital, or 1 per cent of total assets; the provider can access the general ledger or confidential policyholder information; provider failure could interrupt a material line of business or important business service for more than 48 hours; reasonably estimated remediation cost exceeds the same financial threshold; failure could materially damage the entity's or The Bahamas' reputation; or the arrangement affects statutory or regulatory reporting. An entity may rebut the presumption only with a documented assessment approved by the Board and available to the Commission.

5.6. In assessing materiality, a regulated entity shall also consider, at minimum:

- Financial, reputational, and operational impact, with specific reference to significant business lines and the consequences if the service provider fails to perform as agreed;
- Regulatory compliance and internal controls, particularly the entity's ability to maintain effective oversight if the provider experiences difficulties;
- Data access and continuity, including risks of losing access to important data and the difficulty/time required to find an alternative provider or bring the service back in-house;
- Cost implications, both short-term and long-term, including hidden or contingent expenses;
- Internal capacity development, assessing the impact on long-term expertise and resilience;
- Concentration and cross-border risk, including reliance on a single provider and risks associated with providers located outside The Bahamas.

A function or activity shall be deemed material if its disruption (e.g., service failure, security breach, or provider insolvency) could significantly impair the entity's business operations, reputation, profitability, risk management, or compliance with applicable laws and regulations. Materiality assessments shall be reviewed annually and updated immediately upon any material change in the outsourcing arrangement.

Materiality assessments must be documented using the format in **Appendix 1 - Materiality and Criticality Assessment**.

6. Governance and accountability

6.1. The Board retains ultimate accountability for the outsourcing framework. It must:

- approve and annually review the outsourcing and third-party risk policy, risk appetite and materiality methodology;
- approve entry into, material variation of, or exit from each critical or material arrangement, subject to documented delegations for lower-risk arrangements;
- ensure sufficient retained expertise and resources to oversee providers and, where necessary, reintegrate or transfer services;
- review at least quarterly reporting on material arrangements, performance, incidents, concentration, remediation and exit readiness;
- ensure conflicts of interest, including in intra-group arrangements, are identified and managed; and
- ensure outsourcing does not compromise the independence or effectiveness of a control function.

Boards must provide annual attestation in the format of **Appendix 6 - Annual Board Attestation**.

- 6.2.** Senior management must implement the Board-approved framework, assign an accountable owner for each arrangement, maintain the register, ensure cross-functional review by risk, compliance, legal, cybersecurity, data protection and internal audit as relevant, and escalate material matters promptly.
- 6.3.** Internal audit must provide risk-based independent assurance over the design and operating effectiveness of the outsourcing framework. It must have unrestricted access to relevant records, systems, personnel and providers.

7. Outsourcing policy and lifecycle framework

- 7.1.** The entity must maintain a written policy covering identification, classification, approval, due diligence, contracting, implementation, monitoring, incident management, renewal, material change and exit.
- 7.2.** The policy must define roles, delegated authorities, risk acceptance, prohibited arrangements, documentation standards, reporting frequencies, notification triggers and controls for cross-border, cloud, intra-group and sub-outsourcing arrangements.
- 7.3.** No business unit may commit to a material outsourcing arrangement before completion of the required risk assessment, due diligence, approvals and contract review.

8. Pre-outsourcing risk assessment

- 8.1.** Before entry, renewal or material change, the entity must document the business case and assess at least:
 - strategic, operational, financial, legal, regulatory, conduct, reputational and policyholder risks;
 - cybersecurity, privacy, data location, data sovereignty, access, integrity, availability and recoverability;
 - provider, sectoral, geographic and systemic concentration;
 - substitutability, lock-in, transition time, skills and resources required for exit;
 - country, geopolitical, sanctions, legal-enforceability and cross-border transfer risk;
 - sub-outsourcing depth and supply-chain dependencies;
 - impact on important business services, recovery objectives and maximum tolerable disruption;
 - aggregate exposure across the group and across services relying on the same provider; and
 - whether the arrangement could impair substance, control-function independence or supervisory access.
- 8.2.** The assessment must identify inherent risk, controls, residual risk, accountable owners, approval authority and risk-acceptance rationale. Material assessments must be approved by the Board or an appropriately mandated Board committee.

9. Due diligence

- 9.1.** Due diligence must be completed before appointment and refreshed periodically in proportion to risk, at least annually for critical providers.
- 9.2.** The review must address the provider's ownership, governance, competence, staffing, capacity, financial condition, reputation, regulatory status, litigation and enforcement history, insurance coverage (including adequacy of professional indemnity or cyber liability policies), conflicts of interest

(with disclosure and mitigation measures), strategic alignment with the regulated entity's objectives, and human resource capacity (qualifications, training, and stability of assigned staff), security controls, data practices, business continuity, disaster recovery, incident record, subcontractors and ability to comply with Bahamian requirements.

9.3. For material technology or cloud providers, the entity must assess relevant independent assurance and certifications, including SOC reports, ISO/IEC 27001 or equivalent evidence, while independently evaluating the scope, exceptions and applicability of that assurance.

9.4. Due diligence may not be reduced merely because the provider is within the same group or is a market-dominant provider.

10. Contractual and service-level requirements

10.1. Every material outsourcing arrangement must be governed by a written, legally binding agreement reviewed by appropriately qualified legal counsel and approved under the entity's governance framework.

10.2. The agreement must address, as applicable:

- precise scope, service locations, commencement, duration and responsibilities;
- measurable service levels, key performance and risk indicators, reporting and escalation;
- compliance with Bahamian law, Commission requirements and the entity's policies;
- confidentiality, data ownership, permitted use, access control, encryption, retention, return and secure deletion;
- incident detection and notification to the entity without undue delay and early enough to meet regulatory deadlines;
- business continuity, disaster recovery, recovery objectives, resilience testing and participation in exercises;
- the entity's, its auditors' and the Commission's unrestricted rights of access, information, inspection and audit, including where relevant, access to premises, systems, personnel and subcontractors;
- cooperation with the Commission and production of records in a usable form without delay;
- conditions for sub-outsourcing and advance notice of material changes;
- fees, remedies, service credits, indemnities, liability, insurance and dispute resolution;
- ownership and portability of data, applications, configurations and documentation;
- change management and obligations on acquisition, restructuring, insolvency or control change;
- termination rights, transition assistance, step-in rights where appropriate, and continued service during transition; and
- survival of confidentiality, records, access, audit and cooperation obligations after termination.

Every material outsourcing agreement must expressly state that the governing law is that of The Bahamas, require the service provider to maintain adequate insurance coverage (including professional indemnity and cyber liability policies), and contain explicit dispute resolution provisions specifying mechanisms for resolving disputes, escalation procedures, and applicable jurisdiction.

10.3. A contractual term must not prevent, restrict, delay or impose unreasonable cost on the entity or the Commission in exercising access, audit, information-gathering, inspection or supervisory rights.

10.4. Each material agreement must include a service level agreement ("SLA") or schedule with objective and measurable service, control and resilience requirements. The SLA must identify the measurement

method, data source, reporting frequency, performance threshold, breach classification, escalation time, remediation deadline, service credit or other remedy, and circumstances requiring invocation of continuity or exit arrangements. Each material agreement must include a service level agreement schedule consistent with **Appendix 5 - Service Level Agreement Schedule**.

- 10.5.** At a minimum, the SLA must address availability, accuracy and completeness, transaction or case-processing times, claims or customer-service turnaround where relevant, incident acknowledgement and resolution, recovery time and recovery point objectives, security and vulnerability remediation, regulatory information production, backup success and restoration testing, change management, capacity, complaint handling, and timely notification of subcontractor or location changes.
- 10.6.** Service credits or financial remedies must not be treated as a substitute for remediation, risk mitigation, policyholder redress, notification to the Commission, or exercise of termination rights.

11. Data, cybersecurity, cloud and cross-border arrangements

- 11.1.** Outsourced and third-party services must be governed within the entity's Cyber Risk Management Framework and comply with the Commission's Cybersecurity Risk Management Guidance and the Data Protection Act, Ch. 324A.

In addition, outsourcing agreements must include explicit contractual safeguards to ensure confidentiality and data protection, cross-referenced with Section 11. Specifically:

- Contracts must contain explicit confidentiality provisions binding service providers and subcontractors to protect customer information to the same standard as the regulated entity.
- Service providers must not disclose customer information to subcontractors or third parties without prior written consent of the regulated entity and notification to the Commission.
- Contracts must prohibit service providers from using proprietary or customer information except where necessary to provide the contracted service.
- Contracts must require service providers to promptly notify the regulated entity and the Commission if disclosure of customer information is compelled by law or judicial authority, subject to applicable law.
- Outsourcing arrangements must include provisions requiring service providers to identify, disclose, and effectively manage conflicts of interest, with mitigation measures overseen by the Board and subject to supervisory transparency.

- 11.2.** The entity must maintain an inventory and classification of data accessed, processed, transmitted or stored by providers; apply least-privilege access, strong authentication and encryption; monitor access and anomalous activity; and ensure timely revocation of access.
- 11.3.** Where data or processing is outside The Bahamas, the entity must assess destination-country law, enforceability, foreign-authority access, data sovereignty, transfer restrictions and whether comparable protection is maintained. Data must remain accessible, recoverable and producible to the Commission regardless of location.
- 11.4.** For material cloud arrangements, contracts and controls must address shared-responsibility allocation, tenant isolation, encryption and key management, availability and security service levels, backup, portability, inter-operability, exit testing, secure deletion and concentration risk.
- 11.5.** A material cybersecurity incident affecting an outsourced service must be notified to the Commission as soon as practicable and no later than 72 hours after detection, without waiting for complete investigation. Significant updates and a root-cause and remediation report must follow.

12. Sub-outsourcing

- 12.1. The entity must identify material subcontractors and retain contractual authority to approve, object to or require risk mitigation for material sub-outsourcing.
- 12.2. The primary provider must remain responsible for subcontractor performance and must flow down equivalent confidentiality, security, resilience, access, audit, incident, record-retention and termination obligations.
- 12.3. The entity must assess cumulative risk across the full service chain and ensure that sub-outsourcing does not impair oversight, exit or Commission access.

13. On-going monitoring and assurance

- 13.1. The accountable owner must monitor performance and risk throughout the arrangement. Monitoring must include service-level performance, incidents, complaints, control exceptions, financial condition, staffing, location, subcontracting, assurance findings, concentration and regulatory developments.
- 13.2. Critical arrangements must be formally reviewed at least quarterly and material arrangements at least annually. Reviews must be more frequent where risk, performance or change warrants.
- 13.3. Material deficiencies must have documented owners, deadlines and escalation. The entity must verify remediation and consider restriction, suspension, replacement, step-in or termination where risk remains outside appetite.
- 13.4. Independent assurance must be risk-based. Reliance on pooled audits or provider reports is permissible only where their scope, competence, independence, period and findings are adequate and do not restrict the Commission's rights.

14. Business continuity, operational resilience and exit

- 14.1. The entity must map provider dependencies supporting important business services and set Board-approved recovery objectives and impact tolerances.
- 14.2. Business continuity and disaster recovery arrangements must be aligned, tested at least annually for critical services, and tested under severe but plausible scenarios, including cyberattack, provider insolvency, telecommunications failure, natural catastrophe, loss of a key location and simultaneous provider disruption.
- 14.3. Each material arrangement must have a documented, feasible and periodically tested exit strategy covering planned and stressed exit, alternative providers or reintegration, data and application migration, transition resources, communications, regulatory engagement and continuity of policyholder service.

Exit strategies must be documented and tested using the format in **Appendix 9 - Exit Strategy Checklist**.

- 14.4. The entity must not enter an arrangement where no credible exit can be maintained, unless the Board formally accepts the risk and the Commission has been notified and raises no objection.
- 14.5. In addition to the requirements in 14.1-14.4, outsourcing agreements must incorporate the following safeguards:

- Board oversight of transition arrangements: Boards and senior management remain accountable for overseeing transition arrangements to ensure continuity of critical functions and compliance with applicable laws during and after termination.
- Mandatory record retention and access: Business continuity and exit provisions must require the retention of, and ready access to, all records necessary to sustain business operations, meet statutory obligations, and provide such information as may be required by the Commission to exercise its supervisory powers.
- Supervisory transparency: Regulated entities must promptly notify the Commission of transition plans, deficiencies, or exemptions claimed in relation to continuity or exit provisions. The Commission reserves the right to accept, reject, or impose conditions on such exemptions.

15. Intra-group arrangements

- 15.1.** Intra-group outsourcing is subject to the same outcomes and must be documented on terms that permit effective oversight. The assessment may recognize group controls but must address conflicts, dependency, contagion, transfer pricing, local legal enforceability and the local entity's exit options.
- 15.2.** The local Board and senior management remain accountable and must retain sufficient substance, authority, records and expertise in The Bahamas or as otherwise approved by the Commission.

16. Outsourced control functions

- 16.1.** Outsourcing a compliance, internal audit, risk management or actuarial function is material and requires prior written approval of the Commission where required by legislation or another Commission guideline.
- 16.2.** The entity must preserve independence, authority, direct Board access, fitness and propriety, confidentiality, resources and unrestricted access to records and personnel. An outsourced control-function provider must not audit or independently assure its own work.
- 16.3.** An application to outsource the compliance function must satisfy the Commission's Guidelines for the Compliance Function, including submission of the provider's details, evidence of competence, independence, resources and capacity, the Board-approved agreement, and appointment and replacement procedures.
- 16.4.** Where requirements conflict, the stricter applicable requirement prevails.

17. Notifications, approvals and incident reporting

- 17.1.** The entity must notify the Commission in writing at least 10 business days before entering into or materially varying a critical or material outsourcing arrangement, unless a shorter period is accepted by the Commission. Notifications of proposed outsourcing arrangements must be submitted using the format in **Appendix 3 – Outsourcing Approval Form**.
- 17.2.** Prior written approval is required where prescribed by law, licence condition or another Commission guideline, including outsourcing of the compliance function. A notification does not constitute approval or non-objection unless confirmed in writing.
- 17.3.** The Commission must be notified without undue delay of:

- a material service failure, breach, data loss, cyber incident or prolonged disruption;
- a matter likely to materially affect provider performance, including insolvency, enforcement action,
- significant control change or loss of critical personnel;
- a material restriction on access, audit or production of records;
- a material change in service location, data location or sub-outsourcing;
- termination of a material arrangement, with reasons and transition plan; and
- any circumstance that may materially affect policyholders, compliance, financial condition or operational resilience.

17.4. Cyber incidents are subject to the 72-hour outer limit in paragraph 11.5. Other material events must be reported as soon as practicable and ordinarily within two (2) business days of the entity becoming aware of the event, consistent with the Commission's expectations for timely supervisory engagement. A regulated entity must not delay initial notification because impact has not been fully quantified.

17.5. Notifications must contain the information reasonably available at the time and must be supplemented as facts develop. A regulated entity must not delay initial notification because impact has not been fully quantified. Notifications must be submitted using the structured forms prescribed in the appendices, including **Appendix 3 - Outsourcing Approval Form**, **Appendix 8 - Notification of Material Breach Form**, and **Appendix 9 - Exit Strategy Checklist**. These forms must be completed with the information reasonably available at the time and supplemented as facts develop. A regulated entity must not delay initial notification because impact has not been fully quantified."

17.6. Notifications and outsourcing arrangements must explicitly confirm compliance with the Financial Transactions Reporting Act ("FTRA") and the Financial Intelligence Unit Act ("FIU Act"). Regulated entities remain fully accountable for ensuring that outsourced functions do not diminish their obligations under AML/CFT/CPF legislation. Recordkeeping, reporting, and supervisory access requirements under these Acts apply equally to outsourced service providers, and must be documented in contracts and reporting forms.

18. Register and record keeping

18.1. The entity must maintain a complete, current, centralized register of outsourcing and material third-party arrangements in the format of **Appendix 2 - Outsourcing Register Template** or an equivalent format.

18.2. The register must be reviewed at least quarterly, approved by senior management at least annually, and provided to the Board and the Commission on request. The Commission may require periodic submission.

18.2A. An annual summary of all critical and material outsourcing arrangements, together with the attestation in Appendix 6, must be submitted by 30 January for the preceding calendar year, or on another date or through another reporting mechanism specified by the Commission.

18.2B. Regulated entities must also provide annual reporting to the Commission on all outsourcing arrangements involving material functions, including updates on risk assessments, performance monitoring, and material changes.

18.3. Records supporting classification, risk assessment, due diligence, approval, contracting, monitoring, assurance, incidents, resilience tests, outsourcing registers and supporting documentation must be retained for at least seven years after termination, or longer where another law requires, and must be made readily available to the Commission upon request.

19. Commission access and supervisory powers

- 19.1.** The entity must ensure that the Commission can obtain promptly all information necessary to supervise the entity and the outsourced activity, irrespective of provider, jurisdiction, technology, contractual chain or termination.
- 19.2.** The Commission may review policies, registers, assessments, agreements, assurance reports, incidents, tests and exit plans; meet providers; conduct or commission examinations; and require independent assurance.
- 19.3.** Where an arrangement creates undue risk or impairs supervision, the Commission may require enhanced controls, contract amendment, restriction of scope, provider replacement, migration, reintegration, termination or any other lawful remedial action. In addition, the Commission has the explicit authority to direct the termination or modification of outsourcing arrangements where it deems necessary to protect policyholders, market stability or compliance with applicable laws.

20. Transition and consequences of non-compliance

- 20.1.** Existing arrangements must be inventoried and classified within three months of the effective date. Critical and material arrangements must be brought into substantial compliance within 12 months, or earlier where directed by the Commission.
- 20.2.** Where a legacy contract cannot be amended by the transition deadline, the entity must document the gap, risk mitigation, Board-approved remediation and earliest renewal or exit date, and notify the Commission.
- 20.3.** Failure to comply may inform the Commission's risk assessment and result in supervisory directions or enforcement action under applicable legislation, including modification or termination of outsourcing arrangements and the imposition of administrative penalties to deter non-compliance.

Entities should benchmark adoption against the framework in **Appendix 7 - Benchmark Adoption Matrix**.

Appendix 1 – Materiality and criticality assessment

Instruction: Complete before entry, renewal and material change. A “yes” answer does not automatically determine classification; the rationale and aggregate effect must be documented.

In addition to the checklist below, the entity must consider broader criteria including financial strength, reputational impact, operational resilience, data access, cost implications, internal capacity development, concentration, and cross-border risk. These narrative criteria supplement the thresholds and must be documented in the rationale.

Numeric thresholds (e.g., B\$1 million, 5% of regulatory capital, or 1% of total assets) are guidance, not absolutes. Smaller licensees may rebut presumptions of materiality only with a documented assessment approved by the Board and available to the Commission.

#	Assessment question	Response	Rationale / evidence
1	Could disruption materially harm policyholders or market confidence?	Yes / No	
2	Does the service support an important business service or statutory obligation?	Yes / No	
3	Would failure materially affect solvency, liquidity, financial reporting or claims payment?	Yes / No	
4	Does the provider access material volumes of personal, confidential or regulated data?	Yes / No	
5	Is the arrangement a control function or core insurance activity?	Yes / No	
6	Is substitutability low or transition time/cost high?	Yes / No	
7	Is there material provider, geographic, technology or group concentration?	Yes / No	
8	Does the arrangement involve material cloud, cyber, cross-border or sub-outsourcing risk?	Yes / No	
9	Could failure impair the Commission's access or the entity's substance?	Yes / No	
10	Would disruption exceed an approved impact tolerance?	Yes / No	

Proposed classification: Critical / Material / Non-material

Residual risk rating: High / Medium / Low _____

Accountable owner: _____

Approver and date: _____

Next review date: _____

Appendix 2 – Outsourcing register

Field	Required information
Reference	Unique arrangement identifier
Entity / group	Regulated legal entity and relevant group
Service	Description and business owner
Provider	Legal name, group relationship and regulatory status
Locations	Service, data-processing and data-storage jurisdictions
Classification	Critical / material / non-material and rationale
Important service	Supported important business service and impact tolerance
Data	Categories, sensitivity and cross-border transfer
Sub-outsourcing	Material subcontractors and locations
Dates	Contract start, expiry, renewal and notice periods
Approvals	Board/committee and Commission approval or notification dates
Risk	Inherent/residual rating and concentration dependencies
Assurance	Audit/access rights and most recent assurance review
Resilience	RTO/RPO, last test and test outcome
Incidents	Material incidents and open remediation
Exit	Exit owner, strategy, last test and estimated transition period
Review	Last and next review dates

Appendix 2 - Outsourcing Register Template

1. Reference – Unique arrangement identifier

2. Entity / Group – Regulated legal entity and relevant group

3. Service – Description of outsourced function and business owner

4. Provider – Legal name, group relationship, and regulatory status

5. Locations – Service, data-processing, and data-storage jurisdictions

6. Classification – Critical / material / non-material and rationale

7. Important Service – Supported important business service and impact tolerance

8. Data – Categories, sensitivity, and cross-border transfer

9. Sub-outsourcing – Material subcontractors and locations

10. Dates – Contract start, expiry, renewal, and notice periods

11. Approvals – Board/committee and Commission approval or notification dates

12. Risk – Inherent/residual rating and concentration dependencies

13. Assurance – Audit/access rights and most recent assurance review

14. Resilience – RTO/RPO, last test, and test outcome

15. Incidents – Material incidents and open remediation

16. Exit – Exit owner, strategy, last test, and estimated transition period

17.

17. Review – Last and next review dates

Appendix 3 – Outsourcing Approval Form

1. Regulated entity, licence number and contact

2. Type of submission: notification / approval application / material change / termination

3. Description of outsourced function (scope, criticality, materiality classification)

4. Service and business rationale

5. Service and data locations

6. Proposed commencement, duration and renewal

7. Provider, ownership, regulatory status and relationship to entity

8. Classification and completed materiality assessment

9. Important business services and impact tolerances affected

10. Summary of risk assessment and residual risks

11. Due diligence completed and material findings

12. Concentration and sub-outsourcing exposure

13. Data, cyber, privacy, cloud and cross-border safeguards

14. Due diligence findings: governance, competence, insurance coverage

15. Conflicts of interest and mitigation measures

16. HR capacity and stability

17. Business continuity, disaster recovery and latest test

18. Contractual safeguards: governing law, confidentiality, dispute resolution, termination rights, insurance coverage

19. Exit strategy, estimated transition time and alternatives

20. Board/committee approval date

21. Contract confirmation and material deviations from Appendix 4

22. For control functions: independence, fitness, resources, capacity and direct Board access

23. Declaration by CEO or equivalent that information is complete and the entity retains accountability

DRAFT

Appendix 4 – Minimum contractual clauses checklist

Outsourcing agreements must, at a minimum, include the following contractual clauses:

✓	Clause	Location / gap / remediation
☐	Scope of services, service locations, commencement date, duration, and responsibilities of each party	
☐	Measurable service levels, KPIs/KRIs, reporting obligations, and escalation procedures	
☐	Compliance with law and Commission requirements	
☐	Confidentiality provisions, privacy provisions, data ownership, encryption standards, retention periods, permitted data use, and secure deletion requirements	
☐	Security controls, access, encryption and vulnerability management	
☐	Incident detection, notification without undue delay, and remediation obligations	
☐	Data ownership, access, portability, retention, return and deletion	
☐	Business continuity, disaster recovery, resilience testing (including RTO/RPO) commitments and periodic testing).	
☐	Board oversight of transition arrangements to ensure continuity of critical functions and compliance during and after termination	
☐	Mandatory record retention and access provisions to sustain operations and meet statutory obligations	
☐	Supervisory transparency requirements, including notification to the Commission of transition plans, deficiencies, or exemptions	
☐	Name of Auditor, Audit rights, including access for the regulated entity and the Commission	
☐	Provider cooperation with the Commission	
☐	Sub-outsourcing Commission's approval/objection, notice and flow-down	
☐	Change control and notification of adverse developments	
☐	Fees, insurance, liability, remedies and dispute resolution	
☐	Termination for cause, regulatory direction and convenience where appropriate	

✓	Clause	Location / gap / remediation
☐	Step-in and transition assistance	
☐	Continued service during exit	
☐	Survival of confidentiality, records, audit and cooperation terms	
☐	Governing law and enforceability assessment: All outsourcing contracts shall be governed by the laws of The Bahamas. Contracts must also undergo an enforceability assessment to ensure that the governing law clause, insurance obligations, and dispute resolution provisions are legally binding, effective, and capable of being upheld in Bahamian courts.	
☐	Insurance coverage adequacy: Contracts must require the service provider to maintain adequate insurance coverage, including professional indemnity and cyber liability policies, to support its obligations.	
☐	Explicit dispute resolution: Contracts must contain explicit dispute resolution provisions, specifying mechanisms for resolving disputes, escalation procedures, and applicable jurisdiction.	
☐	Explicit contractual confidentiality clauses binding service providers and subcontractors.	
☐	Restrictions on subcontractor or third-party disclosure without prior consent of the regulated entity and notification to the Commission.	
☐	Prohibition on use of proprietary or customer information except for contracted services.	
☐	Notification of legal disclosure requirements to the regulated entity and the Commission.	
☐	Conflict of interest disclosure and mitigation obligations, with Board oversight and supervisory transparency.	

Appendix 5 – Service level agreement schedule

Instruction: Use this schedule as a minimum. Metrics must be tailored to the outsourced service and linked to important business services, risk appetite and impact tolerances.

Service / control	Metric and method	Target / tolerance	Reporting	Escalation / remedy
Availability	Percentage service availability; excluded downtime defined		Monthly	
Processing quality	Accuracy, completeness, rework and error rate		Monthly	
Turnaround	Processing or response time by priority/customer impact		Monthly	
Incidents	Acknowledgement, containment, resolution and notice time		Per incident	
Resilience	RTO, RPO, backup success and restoration test		Quarterly / test	
Cybersecurity	Critical/high vulnerability remediation; access reviews		Monthly	
Regulatory access	Time to produce complete records to entity/Commission		Per request	
Capacity	Utilisation, peak capacity and resource sufficiency		Quarterly	
Complaints	Volume, ageing, upheld rate and root-cause remediation		Quarterly	
Changes	Advance notice, testing, rollback and approval		Per change	
Subcontractors	Advance notice and updated risk information		Per change	
Exit readiness	Data export, portability and transition test outcomes		Annual	

Appendix 6 – Annual Board attestation

For the reporting period ending: _____

Name of registrant/licensee: _____

Annual Corporate Governance Certificate- Outsourcing Oversight

The Board of Directors confirms, after reasonable enquiry, that:

- The entity maintains an outsourcing and third-party risk framework proportionate to its risk profile;
- All known arrangements have been recorded and classified;
- Critical and material arrangements have been risk-assessed, appropriately approved and monitored;
- The Board has reviewed material performance, incidents, concentration risk, resilience and exit readiness;
- Material regulatory notifications and approval applications have been made;
- The Commission's access has not been impaired;
- Exceptions are disclosed below with Board-approved remediation; and
- The Board has fulfilled its obligations under these Guidelines with respect to outsourcing and third-party risk management.

Deficiencies and Action Plan

The Certificate must identify any deficiencies in governance or oversight of outsourcing arrangements and include an Action Plan to the Commission addressing remediation of deficiencies.

Exceptions and remediation:

Chair of the Board: _____ Signature: _____ Date: _____

Chief Executive Officer or equivalent: _____ Date: _____

The Certificate shall be submitted to the Commission together with the annual outsourcing register summary (Appendix 2) by 30 January for the preceding calendar year, or on another date specified by the Commission.

Appendix 7 – Benchmark adoption matrix

Source	Relevant practice	Treatment in draft
Central Bank of The Bahamas – Minimum Standards for Outsourcing of Material Functions (2020)	10-business-day prior notice; quantitative and qualitative materiality indicators; Board approval; SLAs; annual summary; at least triennial risk-based audit; direct supervisory access.	Adopted, with insurance-specific terminology and broader operational-resilience requirements.
Securities Commission of The Bahamas – Securities Industry Regulations / regulatory obligations	Prior notification of proposed outsourcing.	Adopted through prior notice for all critical and material arrangements.
Insurance Commission of The Bahamas – Corporate Governance Guidelines (2026)	Board approval and risk assessment of material outsourcing; written agreements; periodic Board and senior-management reporting.	Embedded throughout governance, risk assessment, contracting and reporting.
Insurance Commission of The Bahamas – Cybersecurity Risk Management Guidance	Full accountability; third-party/cloud due diligence; Board approval for material cloud; breach notification, audit, data security, SLAs, BCP/DRP and exit.	Embedded in sections 10–14 and incident reporting.
Cayman Islands Monetary Authority – Outsourcing SOG and 2026 thematic review	Annual assessments; centralized log; substance; detailed contracts; correction of observed access, insurance, notification and exit gaps.	Adopted.
Bermuda Monetary Authority – Operational Resilience and Outsourcing	Important business services, impact tolerances, mapping, severe-but-plausible testing and resilience lifecycle.	Adopted.
Jamaica FSC – Guidelines for Standard of Conduct for Service Providers	14-day notice; written agreements; due diligence; contingency; prompt termination; no restriction on regulator; regulatory approval for sub-outsourcing in that framework.	Core safeguards adopted; ICB uses risk-based approval/objection rights for material sub-outsourcing.
Barbados FSC – Technology and Cyber Risk Management Guideline	Pre-contract technology/cyber assessment; ongoing high standard of care; rigorous sub-outsourcing diligence; staff/contractor competence and background controls.	Adopted proportionately.
United Kingdom PRA, Canada OSFI, Singapore MAS	Lifecycle governance; criticality; cloud portability; concentration; registers; access; exit.	Adopted.

Drafting and implementation notes (for Commission use)

Not for publication without review: This page records policy choices requiring final confirmation before issuance.

Issue	Recommended position	Final decision
Legal basis	Confirm current External Insurance Act section and whether the 2025/2026 replacement Act has commenced.	
Regulatory engagement	Use 10-business-day notice for critical and material arrangements, aligning with the Central Bank; retain prior approval where another guideline or law requires it.	
Incident timing	Align material cyber incidents to the existing 72-hour requirement; use two business days for other material outsourcing events.	
Scope	Apply across insurers, external insurers, managers and intermediaries, proportionately.	
Legacy contracts	Three months to inventory/classify; 12 months to remediate.	
Submission mechanism	Confirm portal/email and responsible department; draft assumes annual return by 30 January, aligned with the Central Bank's domestic model.	
Public consultation	Consider 45-day consultation with a targeted questionnaire on notification thresholds and proportionality.	

Appendix 8 - Notification of Material Breach Form

1. Regulated entity, licence number and contact

2. Date and time of breach or incident detection

3. Type of breach / incident (service failure, data loss, cyber incident, prolonged disruption, compliance breach, other)

4. Description of event and affected outsourced function(s)

5. Service provider details (name, ownership, jurisdiction, regulatory status)

6. Important business services and impact tolerances affected

7. Initial risk assessment (financial, operational, reputational, compliance, data, concentration, cross-border)

8. Immediate remedial actions taken by provider and entity

9. Residual risks and potential impact on policyholders, operations, or compliance

-
10. Escalation and communication measures (Board, senior management, Commission, policyholders if applicable)

11. Planned remediation steps, timelines, and accountable owners

12. Declaration by CEO or equivalent that information provided is complete to the best of their knowledge and that the entity retains accountability

DRAFT

Appendix 9 - Exit Strategy Checklist

1. Regulated entity, licence number and contact

2. Outsourced function(s) subject to exit

3. Service provider details (name, ownership, jurisdiction, regulatory status)

4. Reason for exit (termination, provider insolvency, regulatory direction, other)

5. Estimated transition time and resources required

6. Alternative providers or reintegration options identified

7. Data and application migration plan (including portability, secure transfer, deletion)

8. Business continuity arrangements during transition

9. Communication plan (Board, Commission, policyholders, staff, other stakeholders)

10. Record retention and supervisory access provisions

11. Board oversight and approval of exit plan

12. Declaration by CEO or equivalent that continuity safeguards are in place and entity retains accountability

DRAFT