



BERMUDA MONETARY AUTHORITY

INSURANCE DEPARTMENT

GUIDANCE NOTE # 17

COMMERCIAL INSURER RISK ASSESSMENT

November 2008

Introduction

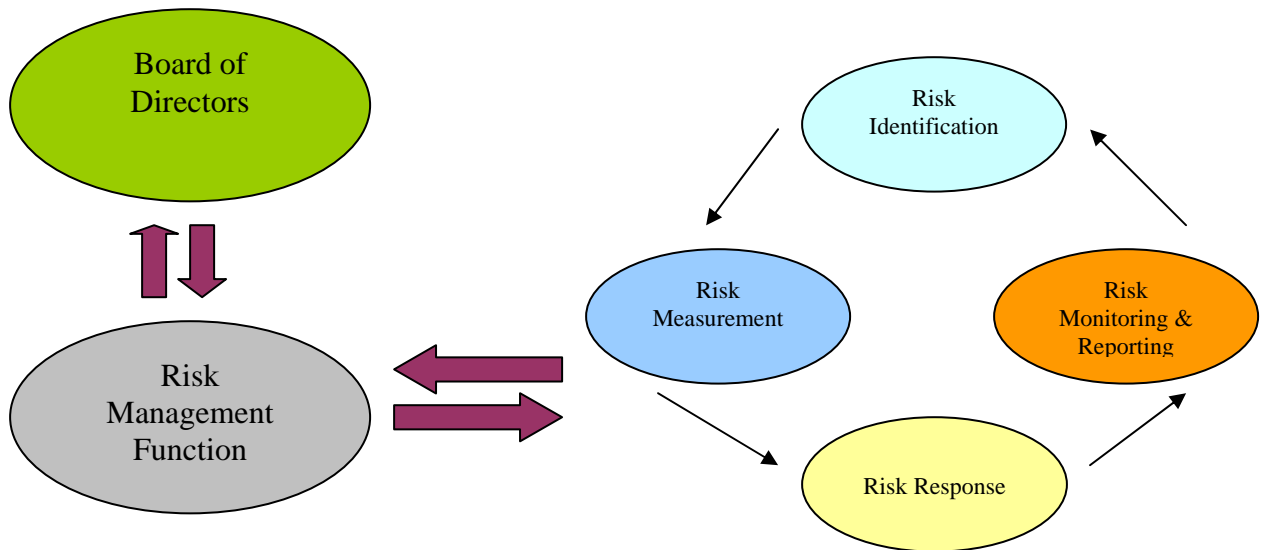
1. The Bermuda Monetary Authority (“the Authority”) is introducing the Commercial Insurer Risk Assessment (“the CIRA” or “the CIRA Framework”), which is to be completed by the Class 4 insurers (“the insurer”), as defined under Section 4 of the Insurance Act 1978 (2008 Consolidated) (“the Act”). In this Guidance, “insurer” also refers to “reinsurer”, and “insurance” also refers to “reinsurance” pursuant to Section 1 of the Act.
2. The CIRA will serve primarily as an assessment tool that will enhance the Authority’s risk-based supervisory framework. The Authority recognises the need for clarity as to the scope and implementation of the CIRA if the regulatory system is to command the confidence of both insurers and policyholders. It seeks, therefore, to ensure that the insurer operating in Bermuda has a good understanding of the nature of the requirements and of the Authority’s approach in implementing the CIRA.
3. While the Authority aims to provide clarity as to its approach, the Guidance is not intended to be exhaustive. The Authority, through the Guidance, hereby sets out its understanding of the CIRA and how the insurer may apply the framework as an assessment of its insurance operations. The Authority will endeavour to communicate this through the Guidance Note and any subsequent revisions, as and where necessary.
4. Other guidelines issued by the Authority may contain additional information related to the CIRA Framework.
5. The Authority’s guidance is of general application and seeks to take account of the wide diversity of institutions that may be licensed under the Act. There may be a need for revision of the Guidance Note from time to time. Material changes in the Guidance Note will be published, generally through the issue of a revised version.

Application

6. The CIRA (see Appendix I) is to be completed by the insurer and submitted to the Authority with the Bermuda Solvency Capital Requirement (“the BSCR”) model as prescribed by the Insurance (Prudential Standards Class 4 Solvency Requirements) Order 2008 (“the Order”).
7. The CIRA Framework assesses the quality of the insurer’s risk management function surrounding its operational risk exposures. Operational risk is the risk of loss arising from inadequate and/or failed internal processes, people, systems and/or external events. Operational risk also includes legal risks. Reputation risks arising from strategic decisions do not count as operational risks.¹

¹ CEIOPS-DOC-23/01: QIS4 Technical Specifications
Commercial Insurer Risk Assessment
Bermuda Monetary Authority
November 2008

8. The CIRA emphasizes the interrelationship between the Risk Management and Corporate Governance functions as seen below:



9. The Board of Directors has an influential role in establishing, inter alia, the strategic direction and risk culture of the insurer. The Authority views the Risk Management function as a critical tool to furnish the Board with the necessary information to make appropriate decisions and assist the insurer’s management in steering the organization forward. The Authority’s guidance on the importance of the effective control over the insurer’s operation requires that “the Board of Directors, along with Management, [be] responsible for suitable prudential oversight of the risk management and internal control systems, strategies and policies.”²
10. The CIRA Framework should encourage the insurer to “implement and maintain sound and prudent risk management policies and systems capable of promptly identifying, measuring, assessing, reporting and controlling [its] risks.”³ The Risk Management function should enable the insurer “to identify all material risks, financial and non-financial, that they face, assess their potential impact and have policies in place to manage them effectively.”⁴
11. The CIRA highlights the standards related to the Corporate Governance and Risk Management functions as they pertain to the oversight of the insurer’s operational risk exposures. The CIRA provides insurers with credit for instituting such standards,

² Ibid pg 4

³ Guidance Note #13 Risk Management and Internal Controls pg 5

⁴ Ibid

including instituting governance at the group level (where such governance covers the operations of the insurer), by completing the Comments section under each operational risk area accordingly.

12. The CIRA is to be signed off by two Directors of the insurer, one of which must be a resident Director, where the insurer has a resident Director on its Board.
13. The Risk Management function within the CIRA has 4 components: Risk Identification, Risk Measurement, Risk Response, and Risk Monitoring & Reporting. The insurer will undertake the self-assessment by answering the questions related to the calibre of its risk management processes in place to address the material risk arising from each operational risk area.
14. The Authority encourages insurers to consistently review and improve upon their risk management practices. The above diagram illustrates the flow of information that moves within the risk management framework, which would ultimately facilitate re-evaluation and improvement of the risk management process.
15. As a result, the CIRA embodies a maturity model approach to identify an insurer's developmental stage with respect to a specific operational risk area. The CIRA rewards the insurer for achieving progress in each risk management area.
16. The CIRA will come into effect on December 31, 2008.

CIRA Framework

17. The Authority views the effective management of an insurer's operational risk as an integral aspect to sound and prudent management of the insurer's operations. The CIRA Framework will assist the Authority in a risk-based assessment of the adequacy of an insurer's processes and controls addressing operational risk exposures.
18. The Authority's supervisory framework is risk-based and will examine the adequacy of the insurer's processes and controls infrastructure around its operational risk exposures vis-à-vis the insurer's risk profile.
19. The CIRA Framework reviews the following 8 operational risk exposures as follows:
 - a. **Business Process Risks** which includes data entry and data processing errors arising from application design misspecifications.
 - b. **Business Continuity Risks** which includes risks that threaten or disrupt an insurer's continuous operations such as risks arising from natural and man-made hazards.
 - c. **Compliance Risks** which includes legal and regulatory breaches.
 - d. **Information Systems Risks** which includes unauthorized access to systems and data, data loss, utility disruptions, software and hardware failures, and inability to access information systems.

- e. **Distribution Channels Risks** which includes inexperienced or incapable brokers/agents.
 - f. **Fraud Risks** which includes intentional misconduct or unauthorized activities such as misappropriation of assets, information theft, forgery, and fraudulent claims.
 - g. **Human Resources Risks** which includes key person risk, unethical staff (not including fraud), inexperienced or incapable staff, training, retention, and communication failures.
 - h. **Outsourcing Risks** which includes communication failures, and incapable outsourcing partners.
20. The CIRA Framework applies the components within the Risk Management function to each operational risk area. The insurer assesses each operational risk area and selects the applicable descriptor under the “Dimension” column that reflects the developmental stage of the insurer’s process surrounding that specific risk area.
21. In order to be credited with the relevant score within the CIRA Framework, the insurer must fulfil the criteria in the “Dimension” column. In its assessment, if the insurer finds itself between stages, the insurer must select the lower stage. The insurer can supplement this selection with additional comments that can be made at the end of each Risk Management function.
22. The total scores for each component within the CIRA Framework are aggregated and produce the pertinent Operational Risk Charge percentage. The Operational Risk Charge can range from 1% to 10%. The relevant Operational Risk Charge percentage is applied to the “BSCR (After Covariance Adjustment)” subtotal in the BSCR Model. The resultant figure is the Operational Risk Capital Charge.

Operational Risk Assessment

23. Depending on the scale and complexity of the insurer’s operations, the Risk Management function should be tailored to ensure that material risks have been clearly identified and addressed so that the insurer’s strategic objectives are not derailed or impeded in any way and the insurer conducts its business in a sound and prudent manner.
24. The CIRA Framework focuses on processes pertinent to the Risk Management function, which should encompass, inter alia:
- a. Policy statements clearly communicating the insurer’s attitude towards the risk exposures and the insurer’s commitment to mitigate the risk exposures;
 - b. Well documented procedures and processes that are accessible to and understood by relevant persons within the organization;

- c. Documented procedures and processes are reviewed periodically to ensure that they remain current and effective, especially if deficiencies or emerging risks are identified;
- d. Training and periodic communication of the documented procedures and processes to ensure that relevant persons can appropriately apply the standards established by the Board and Management;
- e. Effective controls surrounding the procedures and processes to engender reliability and integrity in the Risk Management Framework;
- f. Management periodically evaluates the effectiveness of the procedures and processes to ensure that they are understood, implemented and are accomplishing the desired effect;
- g. Effective feedback mechanism is established to enable the review of the procedures and processes and to identify any deficiencies within the system that need to be addressed. This would include the appropriate response or action plan, where necessary, based on the feedback received;
- h. Techniques and requisite skills to capture and analyze data and/or information as it pertains to operational risk exposures, the repercussions on the organization's goals and objectives and the resultant effects as the organization implements its Risk Management Framework;
- i. Management communicates to the Board periodically on operational risk exposures and the effectiveness of the Risk Management Framework in addressing material risks arising from these areas;
- j. Independent examination of the procedures and processes to verify adherence, reliability and integrity in the Risk Management Framework.

25. The CIRA Framework analyzes the implementation of the afore-mentioned procedures and processes. Each operational risk area should have effective and appropriate implementation of processes and procedures. The effectiveness of the implementation process is determined by the internal control mechanisms engineered around the various operational risk areas.

26. The Authority does not wish to provide exhaustive criteria to assess each operational risk area, since insurers vary in nature, scale and complexity. The Authority has, however, taken a principles-based approach whereby the insurer's Corporate Governance function is responsible for demonstrating to the Authority that the assessment is appropriate for the insurer's operations.

27. Implementing the risk management processes and procedures may incorporate the following actions:

- a. **Business Process Risks** – systems configured to flag when incorrect data is entered, second review of information entered and sign-off, risk acceptance approval limits are communicated and enforced, checklists to ensure that the processes are followed, logging system to receive and distribute correspondence, complaints handling, documentation to support risk acceptance/rejection etc.

- b. **Business Continuity Risks** – remote access facilities with copies of claims and application forms, remote facilities to access information systems in the event of a disaster, emergency power supply, staff evacuation plan, backup media placed in fire-proof vault or offsite, scan documents and store offsite, establish disaster recovery plans along with disaster recovery teams with assigned team leaders, emergency response teams with contact information of essential services etc.
- c. **Compliance Risks** – assign person(s) to review legislative/regulatory requirements to operate in jurisdiction(s), ensure legal or compliance team sign-off for any issues outside the scope of the procedures, legal or compliance team review and sign-off before entering any contractual arrangements or amendments to application forms and/or policy contracts, ensure the proper disclaimers have been communicated etc.
- d. **Information Systems Risks** – update and run security virus scans, key applications are properly tested prior to implementation, authorized personnel have access to computer facilities, authorization to override functions within the programs, maintenance and physical checks on computer systems etc.
- e. **Distribution Channels Risk** – service agreements detailing delegation of authority, ensure intermediaries are licensed to conduct insurance business in jurisdiction(s), review applications and risks to ensure business is congruent with insurer’s risk acceptance criteria, review intermediaries’ marketing strategy to ensure appropriate messages are communicated, training specific to insurance policies, ensure intermediaries have risk management systems in place (especially disaster recovery so as to service policyholders), ensure intermediaries are adequately resourced, monitor customer call centres by conducting spot checks etc.
- f. **Fraud Risks** – produce and propagate an ethics policy, whistle blowing mechanism, background checks on employees, security checks, segregation and/or rotation of duties, confidentiality agreements, proper documentation surrounding ex-gratia claims payments, cheque or other disbursement authorization limits etc.
- g. **Human Resources Risks** – background checks of employees, succession planning, ensure employment practices comply with labour union agreements or/and legislation, insurer communicates its policy on tolerance limits for certain aberrant behaviours, an easily understood and updated employee manual, workplace safety – premises inspection, proper lighting etc.
- h. **Outsourcing Risks** – Conduct due diligence on outsourcing partners, ensure service agreements communicate exactly what the outsourcing partner is required to deliver, confidentiality agreements, outsourcing partners comply with relevant legislation(s), mutually agreed performance and quality standards, establish communication frequency and periodic deliverables, alternative dispute resolution options and jurisdiction clause or service of suit clause in service contracts etc.

Enhanced Capital Requirement

28. The CIRA will assist the Authority in concluding the appropriateness of the Operational Risk Charge being used by the insurer for the purposes of determining its Enhanced Capital Requirement (“the ECR”)⁵ as described in the Order.
29. A re-assessment difference in the Operational Risk Capital Charge by the Authority qualifies as a capital add-on, pursuant to Section 6D of the Act, and will be included in the Authority’s determination of any ECR.

Onsite Supervisory Review

30. The CIRA will also form part of the Onsite supervisory process which will complement the Authority’s examination of the insurer’s operational processes and related risk exposures.
31. The insurer should retain documentation supporting its assessment in the event such documentation is requested for inspection by the Authority’s Onsite function.
32. Credit claimed by insurers will be substantiated during the Onsite supervisory review. Where there is a difference of opinion in a given assessment Dimension or framework area, the Authority will notify the insurer. The Authority will also give reasons for its opinion.
33. The Authority’s reassessment of a given operational risk area will remain in effect for all subsequent filings of the CIRA until such time as the insurer has satisfied the Authority that the developmental stage of that area has sufficiently improved to require a change and the insurer has received written notification from the Authority to alter the reassessment. The adjustment or charge, based on the Authority’s assessment, will come into effect at least 90 days from the date of notification or an extended period as the Authority may determine.
34. The Authority will apply all changes prospectively from the date of notification.

Appeals Process

35. The Authority supports due process and has introduced an appeals process for insurers having a difference of opinion where the Authority has re-assessed the insurer’s Operational Risk Charge.
36. Where the Authority has notified the insurer of a difference of opinion, the insurer will be given 28 days to appeal the decision to the Authority’s in-house Risk

⁵ ECR means additional capital and surplus requirement imposed by or under an Order made under Section 6A of the Act.

Committee (“the Committee”). The adjustment or charge will not come into effect until the Committee has completed its review and rendered a decision.

37. Should the insurer decide that it will not appeal the decision rendered by the Committee, the adjustment or charge will come into effect at least 90 days after the date of notification of the Committee’s decision or an extended period as the Authority may determine.
38. The insurer may appeal before a Tribunal pursuant Section 44A of the Act if it is aggrieved by the Committee.

APPENDIX I

CORPORATE GOVERNANCE

The insurer is to review the following statements below. The insurer is to place an “X” in the column “Implemented” where the Corporate Governance function meets the criteria (200 points for each fulfilled criteria). The worksheet will automatically aggregate all scores.

The Board of Directors:

Dimension	Implemented	Score
Sets risk policies, practices and tolerance limits for all material foreseeable operational risks at least annually and ensures they are communicated to relevant business units		0
Monitors adherence to operational risk tolerance limits more regularly than annually		0
Receives, at least annually, reports on the effectiveness of material operational risk internal controls as well as management’s plans to address related weaknesses		0
Ensures that systems and/or procedures are in place to identify, report and promptly address internal control deficiencies related to operational risks		0
Promotes full, open and timely disclosure from senior management on all significant issues related to operational risk		0
Ensures that periodic independent reviews of the risk management function are performed and receives the findings of the review		0
		0

Comments (optionally, the insurer may provide comments in the box below to support its responses above):

RISK MANAGEMENT FUNCTION

The insurer is to review the following statements below. The insurer is to place an “X” in the column “Implemented” where the Risk Management function meets the criteria (150 points for each fulfilled criteria). The worksheet will automatically aggregate all scores.

The Risk Management Function:

Dimension	Implemented	Score
Is independent of other operational units and has direct access to the Board of Directors		
Is entrenched in strategic planning, decision making and budgeting process		
Ensures that the risk management procedures and policies are well documented and approved by the Board of Directors		
Ensures the risk management policies and procedures are communicated throughout the organization.		
Reviews operational risk management processes and procedures at least annually		
Ensures that loss events arising from operational risks are documented and loss event data is integrated into enterprise risk management		
Documents its risk management recommendations for operational units, ensures that deficiencies have remedial plans and progress on the execution of such plans are reported to the Board of Directors at least annually		

Comments (optionally, the insurer may provide comments in the box below to support its responses above):

RISK IDENTIFICATION

The insurer is to answer the following question. If the answer to the question is "No" then the insurer does not have to complete the matrix/grid. If the answer to the question is "Yes" then the insurer is to identify the stage of progression of each Operational Risk Area based upon the Dimension descriptor. The insurer is then to input an "X" in the grid corresponding to the stage in the matrix table under the relevant Operational Risk Area.

Has your company taken steps to identify material risks arising from the Operational Risk Areas identified below? (Y/N). If "Y", identify the stage of each Operational Risk Area and input an "X" in the appropriate grid under each area.

Risk Identification Processes are:

Progression		Dimension	Operational Risk Areas								Total (Σ)
Stage	Scoring		Fraud	Human Resources	Outsourcing	Distribution Channels	Business Processes	Business Continuity	Information Systems	Compliance	
1	50	"ad hoc"									
2	100	Implemented but not standardized across the organization									
3	150	Implemented, well documented policies and procedures that are understood by relevant staff, and standardized across the entire organization									
4	200	In addition to Stage 3, processes are reviewed at least annually with the view to assessing effectiveness and introducing improvements									
			0	0	0	0	0	0	0	0	0

RISK MEASUREMENT

The insurer is to answer the following question. If the answer to the question is "No" then the insurer does not have to complete the matrix/grid. If the answer to the question is "Yes" then the insurer is to identify the stage of progression of each Operational Risk Area based upon the Dimension descriptor. The insurer is then to input an "X" in the grid corresponding to the stage in the matrix table under the relevant Operational Risk Area.

Has your company taken steps to measure material risks arising from the Operational Risk Areas identified below? (Y/N). If "Y", identify the stage of each Operational Risk Area and input an "X" in the appropriate grid under each area.

Risk Measurement Processes are:

Progression		Dimension	Operational Risk Areas								Total (Σ)
Stage	Scoring		Fraud	Human Resources	Outsourcing	Distribution Channels	Business Processes	Business Continuity	Information Systems	Compliance	
1	50	"ad hoc"									
2	100	Implemented but not standardized across the organization									
3	150	Implemented, well documented policies and procedures that are understood by relevant staff, and standardized across the entire organization									
4	200	In addition to Stage 3, processes are reviewed at least annually with the view to assessing effectiveness and introducing improvements									
			0	0	0	0	0	0	0	0	0

RISK RESPONSE

The insurer is to answer the following question. If the answer to the question is "No" then the insurer does not have to complete the matrix/grid. If the answer to the question is "Yes" then the insurer is to identify the stage of progression of each Operational Risk Area based upon the Dimension descriptor. The insurer is then to input an "X" in the grid corresponding to the stage in the matrix table under the relevant Operational Risk Area.

Has your company taken steps to control and/or mitigate material risks arising from the Operational Risk Areas identified below? (Y/N). If "Y", identify the stage of each Operational Risk Area and input an "X" in the appropriate grid under each area.

Risk Response Processes are:

Progression		Dimension	Operational Risk Areas								Total (Σ)
Stage	Scoring		Fraud	Human Resources	Outsourcing	Distribution Channels	Business Processes	Business Continuity	Information Systems	Compliance	
1	50	"ad hoc"									
2	100	Implemented but not standardized across the organization									
3	150	Implemented, well documented policies and procedures that are understood by relevant staff, and standardized across the entire organization									
4	200	In addition to Stage 3, processes are reviewed at least annually with the view to assessing effectiveness and introducing improvements									
			0	0	0	0	0	0	0	0	0

RISK MONITORING & REPORTING

The insurer is to answer the following question. If the answer to the question is "No" then the insurer does not have to complete the matrix/grid. If the answer to the question is "Yes" then the insurer is to identify the stage of progression of each Operational Risk Area based upon the Dimension descriptor. The insurer is then to input an "X" in the grid corresponding to the stage in the matrix table under the relevant Operational Risk Area.

Has your company taken steps to monitor and report material risks arising from the Operational Risk Areas identified below? (Y/N). If "Y", identify the stage of each Operational Risk Area and input an "X" in the appropriate grid under each area.

Risk Monitoring & Reporting Processes are:

Progression		Dimension	Operational Risk Areas								Total (Σ)
Stage	Scoring		Fraud	Human Resources	Outsourcing	Distribution Channels	Business Processes	Business Continuity	Information Systems	Compliance	
1	50	"ad hoc"									
2	100	Implemented but not standardized across the organization									
3	150	Implemented, well documented policies and procedures that are understood by relevant staff, and standardized across the entire organization									
4	200	In addition to Stage 3, processes are reviewed at least annually with the view to assessing effectiveness and introducing improvements									
			0	0	0	0	0	0	0	0	0

OPERATIONAL RISK CHARGE CALCULATION INSTRUCTIONS

Subject to the Authority applying a re-assessment upon onsite inspection, the “Total Operational Risk Capital Charge” below will be applied to the insurer’s BSCR (After Covariance Adjustment) sub-total in the BSCR model for purposes of arriving at its Enhanced Capital Requirement for the year-end filing.

Overall CIRA Score **0**

CIRA Scoring Grid

OVERALL SCORE	APPLICABLE OPERATIONAL RISK CHARGE % OF "BSCR AFTER COVARIANCE ADJUSTMENT"
≤ 5200	10%
> 5200 ≤ 6000	9%
> 6000 ≤ 6650	8%
> 6650 ≤ 7250	7%
> 7250 ≤ 7650	6%
> 7650 ≤ 7850	5%
> 7850 ≤ 8050	4%
> 8050 ≤ 8250	3%
> 8250 ≤ 8450	2%
> 8450	1%

"BSCR After Covariance Adjustment"

Operational Risk Charge % (Decimals): **10%**

Total Operational Risk Capital Charge: **\$ -**

Director’s Signature:

Print Name:

Date:

Director’s Signature:

Print Name:

Date:

Insurer Name:

Year-end:

Insurer Registration No.

End of Guidance Note.

If you have questions on this or other guidance from the Policy, Research & Risk Assessment Department please email policy@bma.bm . Please put “Insurance Guidance” in the title of your email.