

BERMUDA COMMERCIAL BANK LIMITED

BCB

BERMUDA COMMERCIAL BANK LIMITED

Table of Contents

Background	3
Scope of Application	4
Capital Structure	5
Capital Adequacy	6
Risk Management and Control Framework Overview.....	7
Risk Management and Control Principles.....	7
Risk Management and Control Responsibilities	7
Risk Management and Control Framework.....	8
Credit Risk	8
Securitization	9
Market Risk in Trading Book	9
Stress Testing	10
Liquidity Risk	11
Concentration Risk.....	12
Compliance Risk	14
Operational Risk.....	15
Operational Risk Assessment.....	16
Data Security	17
Internal Audit	18
Human Resources	18
Basel II	19

Background

The disclosure and analysis provided in this document are for the Bermuda Commercial Bank Limited (BCB) which is incorporated in the island of Bermuda as a limited liability company. It is intended to be read in conjunction with the relevant Annual Audited Financial Report which includes important details about the Banks capital adequacy, risk management, and other information.

BCB's accounting policies conform to standards of Bermuda and Canada. In the near future the Bank will change its accounting standards to IFRS (International Financial Reporting Standards).

These disclosures are solely in the context of the local regulatory requirements and guidelines outlined by the Bermuda Monetary Authority under Pillar 3 "Market Discipline of New Capital Adequacy Framework (commonly referred to as Basel II, Pillar 3). The Pillar 3 disclosures have been designed to complement the minimum capital requirements in Pillar 1 as well as the Supervisory Review and Evaluation Process in Pillar II. The accepted aim of Pillar III is to promote market discipline by allowing market participants access to information of risk exposures and risk management policies and process adopted by the Bermuda Commercial Bank Limited.

The Bermuda Commercial Bank's story begins more than 40 years ago, when a group of Bermudan entrepreneurs conceived of forming a local savings and loan institution in Bermuda. The bank has evolved to become the only Bermudian Bank focused on servicing the local and international corporate and commercial business communities as well as high net worth clients. The bank has mastered the art of banking providing the highest standards of service to clients worldwide. The Bermuda Commercial Bank has been guided by a corporate philosophy centered on the provision of innovative, quality service with minimal risk tailored to the specific needs of its clients.

The management of risk is an important criterion to all users of financial services. The Bank has established a policy of minimizing its own corporate risk by following an extremely conservative policy in balance sheet management. The Bank does not take risk positions on its own accounts and runs a matched book policy with its deposits and follows other principles and policies on risk management which is aligned to local Bermuda Monetary Authority regulations wherever required.

Scope of Application

The new capital adequacy framework implemented in Bermuda applies to the Bermuda Commercial Bank Limited (BCB) and its subsidiaries.

BCB is incorporated in the island of Bermuda with limited liability. The Bermuda Commercial Bank Limited has four wholly-owned and controlled subsidiaries; International Corporate Management of Bermuda which provides fund administration and global custody services, BCB Trust Company Limited, Bercom Nominees Limited and BCB (Mauritius) Limited. These subsidiaries are subject to consolidation requirements under the generally accepted accounting principles (GAAP) for Bermuda and Canada and under the capital adequacy framework.

The Bank and its subsidiaries are subject to annual audit by an external audit firm and the Annual Financial Report is published and distributed in hard copy and on the BCB website. Further, the Bank and its subsidiaries are subject to supervisory oversight and onsite inspection by the BMA.

Capital Structure

The capital structure of the Bank comprises of (a) Tier 1 capital which includes Share Capital, Retained Earnings and Share Premium and (b) Tier 2 general provisions/ general loan-loss reserves.

Composition of Capital as at March 31 2010

Tier 1 Regulatory Capital

Ordinary shares/common stock (issued and paid up)	15,246,449
Share premium account	19,847,690
Disclosed prior years reserves etc	38,903,419
Current year's losses	(1,466,899)
	<hr/>
	72,530,659

Total Tier 1 Capital

Tier 2 Regulatory Capital

General provisions (eligible for inclusion)	20,000
	<hr/>
Total Tier 2 Capital	20,000

72,550,659

Total Tier 1 & 2 Capital

Total Capital Deductions

0

72,550,659

Total Eligible Capital Base

Capital Adequacy

Sufficient capital must be in place to support business activities, according to both the Bank's internal assessment and the requirements of the Bermuda Monetary Authority. The key to capital adequacy management is to ensure the compliance with the minimum regulatory capital requirements and targeted capital ratios.

Bermuda Commercial Bank's goal is to maintain sound and optimum capital ratios at all times and therefore not only constantly reviews the present situation but also any projected developments in both its capital base and capital requirements. The main source of the Bank's supply of capital is shareholder investment and retained earnings.

The capital management process is based on the following steps:

- The monitoring of the regulatory capital and ensuring that the minimum regulatory requirements and the established internal targets are met.
- The estimation of the capital requirements based on ongoing forecasting and strategic planning
- The reporting of the regulatory capital situation to both the Senior Management Group and the Bermuda Monetary Authority.

The responsibility for performing these steps is vested in the Asset and Liability Committee (ALCO).

The Chief Operating Officer, the Chief Financial Officer together with the General Manager of Banking are members of ALCO. Internal Audit serves in an advisory capacity to ensure that all parties are keep up to date on the Basel II changes.

Risk Management and Control Framework Overview

Risk Management and Control Principles

There are five key principles that govern Bermuda Commercial Bank's risk management and control framework.

1. Each Manager of the various business units are accountable for operational risk within their unit
2. There is an independent review and reporting of risk through the Internal Audit function
3. There is adequate disclosure of risk
4. Protection of earnings, capital, and deposits is key
5. Protection of the Banks reputation is key

Risk Management and Control Responsibilities

The key entities concerned with risk and control are ALCO, the Risk Committee, Compliance, and Internal Audit.

The Asset and Liability Committee (ALCO) is tasked with determining Bermuda Commercial Bank's fundamental approach to market, credit, interest rate, and liquidity risk. ALCO also has a strategic and supervisory function within the organization when it comes to management and control of such risk at the Bank. ALCO is also responsible for Balance sheet management.

The Internal Audit function provides an independent review, testing, and reporting function for all types of risk. This function reports to the Audit Committee of the Board of Directors.

It is important to note that the head of each business division is accountable for the financial results and risk for their division as well as ensuring that the Bank's policies and procedures related to risk are maintained.

The Risk Committee is primarily concerned with operational risk which encompasses operational controls, data systems integrity, and incident management. The members of the Risk Committee include the Chief Operating Officer, Chief Information Officer, and the Compliance Manager. This committee reports to the Board of Directors through the Chief Operating Officer.

The Compliance function manages the development, implementation, and maintenance of policy and procedure for the relevant regulatory and legislative controls, including Anti-Money Laundering and Know Your Client (KYC) requirements.

The Chief Operating Officer and the Chief Financial Officer are responsible for the overall development and implementation of appropriate control frameworks with support from the business divisions.

The Chief Operating Officer and the Chief Financial Officer are responsible for ensuring that all financial data concerning the performance of the various divisions and subsidiaries are disclosed in a clear and transparent way and that the methodology for reporting adheres to the established regulatory requirements and corporate governance standards as required by the laws and practices of Bermuda. They are also further responsible for the implementation of the Bank's agreed risk management and control framework in the areas of capital management, liquidity funding and tax if applicable.

Risk Management and Control Framework

Bermuda Commercial Bank's risk management and control objectives are implemented within the organization based on a risk management & control framework using policies and quantitative components. This framework is dynamic and is continuously enhanced and adapted as both the banks business and the market and general banking environment evolves.

There are five established key elements in the banks independent risk control framework.

1. Risk policies and procedures
2. Risk identification
3. Risk evaluation
4. Risk control and mitigation
5. Risk and incident reporting

Credit Risk

Credit or Counterparty Risk refers to the risk that a counterparty might fail causing a loss of the banks assets. This risk exists where there is any transfer of value from the bank to other parties, be it in the shape of a loan or a deposit.

The Bank does not generally offer loans or other such credit facilities to clients.

The Bank offers a Letter of Credit product that is fully cash collateralized and is processed through the Bank's correspondent relationship with Deutsche Bank New York.

The Bank is exposed to credit risk when it places fund with other banks or when it purchases investment instruments such as bonds or places monies with money market funds. The size of these deposits are limited by both the Banks internal risk policies and by the Large Exposure limits required by the BMA.

Criteria imposed by the Bank’s internal policies limits investment or placement to high-grade, low-risk instruments and counterparties.

The Bank remains compliant with the Large Exposure limits required by the BMA for money market funds and place no more than the equivalent of 25% of its capital in any single fund or instrument.

Overnight and short-term deposits with counterparty banks are limited as follows;

Fitch Individual Rating	Fitch Short Term rating	Moodys Short term Rating	Maximum Deposit
A or A/B	F1+	P-1	\$60,000,000
B	F1+	P-1	\$50,000,000
B/C	F1+	P-1	\$30,000,000
C	F1+	P-1	\$5,000,000

Over reliance on ratings is not prudent and the Bank also monitors Credit Default Swap 5 year Senior notes (CDSS) spread data. The CDS spreads have proven to be a good indicator of consensus of the risk associated with institutional default.

Asset placement by the Dealing Room is limited to entities on the Approved Instruments List. This list may only be changed by ALCO, subject to quality criteria approved by the Board

Securitization

The Bank has not undertaken any securitization deals during this current period.

Market Risk in Trading Book

Market risk is the risk of loss from changes in the trading market that reduce the value of the Banks investments. The traditional four areas of market risk are Equity Risk (adverse price movement in equity holdings), Interest Rate Risk (adverse movement in interest rates), Currency Risk (adverse movements in foreign exchange rates), and Commodity Risk (adverse changes in commodities holdings).

Currency Risk: The Bank holds no foreign exchange positions on its own behalf, and matches the currency of deposits and capital with corresponding holdings with other banks.

Commodities Risk: The Bank holds no commodities on its own behalf.

Interest Rate Risk: This risk occurs from a mismatch of interest rates, or where an adverse movement in interest rates causes a mismatch. The Bank uses a matched book for term deposits and overnight deposits and offers no other products where rate movement would have an adverse impact.

Equity Risk: The Bank holds a limited position in Bermuda Government guaranteed securities. The total value of these securities at fiscal year end September 30th, 2009 is \$12,690,000. The Bank uses mark-to-market to value these available-for-sale holdings.

Price Risk: Like many banks, the Bank is exposed to price in terms of the interest earned on its deposits with other banks and money market fund holdings. These cash and cash-equivalent holdings generate interest income for the Bank which is impacted by downward changes in the Federal Reserve (FED) rate and the London Interbank Offered Rate (LIBOR).

Given the current business model price risk is the banks single greatest exposure. Price risk arises from the combination of deposit levels, deposit type mix, and interest rate. The factors are;

- Deposit levels in call accounts (non-interest bearing, the bank keeps the overnight rate)
- Deposit levels in term deposits (interest bearing, the bank earns a spread)
- Interest rates paid on DWOBs, the bulk of which is USD and is tied to the FED rate
- Interest rates paid on MMF's which typically lag 3 months behind the FED rate

The highly conservative investment policy fundamentally drives the reliance on interest-sensitive instruments. It reduces the likelihood of counterparty default and losses through the use of deposits with other banks and money market funds, but means that the Bank's income is exposed to adverse changes in interest rates. As the FED rate and LIBOR rates change so does the Bank's interest income.

As of this writing the FED and LIBOR rates remain at historic lows and this has had an impact on the Banks earnings (please refer to the Annual Financial Report 2009 for details).

Stress Testing

The purpose of stress testing is to quantify exposure to extreme and unusual market movements. The Bank's objectives in stress testing are to review a number of possible outcomes, and to provide a control framework that is not only comprehensive but transparent and responsive to the rapidly changing market conditions that it operates in. The Bank performs stress testing on a quarterly basis.

Liquidity Risk

Liquidity Risk exists where demand from clients to withdraw funds from their accounts exceeds the cash available for withdrawal. For example, a liquidity mismatch and risk would exist if the Bank locked up too much money in long-term deposits but offered clients the ability to withdraw their funds on demand (this example also illustrates the concept of 'option risk' where the client has the option of a transaction that could cause a mismatch or impact revenues adversely. Option risk is typical in lending where the client may chose to prepay or make unscheduled balloon payments).

The Bank manages liquidity risk through a 'matched-book' approach whereby the maturity of the client deposit is matched by the counterparty maturity. For example, if a client places \$10m on a 30-day fixed deposit the Bank will place those funds in a 30-day instrument.

The typical profile for fixed and demand accounts is 43% term and 57% demand.

These term deposits can be broken if the client so requires. In general terms the Bank can unwind its portfolio of term deposits in short order with a penalty fee.

Further, the Bank uses daily dealing money market funds and overnight deposits with other banks for its demand balances.

Management uses various reports such as a maturity ladder, fixed deposit maturity schedule and others to forecast flow requirements.

The details of the liquidity maturities are provided in the Audited Financial Report for 2009.

Concentration Risk

Concentration risk arises in various parts of the banks balance sheet and revenue stream. Examples of concentration risk include;

- Reliance on too few or closely related forms of revenue that expose the profitability of the bank to risk from adverse movement in income
- Too few, large clients exposing the balance sheet to risk of material and disproportionate reduction should a small number of clients leave the bank
- Reliance on too few industry sectors (either as clients or as investments) exposing the bank to income or balance sheet risk where a sector experiences adverse business

Given the small size of the Bank there is concentration risk in the client portfolio. Concentration risk for revenues is discussed in the section on Price Risk.

Industry concentration risk exists in that the Bank serves primarily the corporate and commercial sectors. While the client mix is generally diverse the large balances tend to be held by our fund clients. During the recent global recession these clients all experienced reduced subscription and higher levels of redemptions that drove down the fund asset base (reducing fee income in some cases) and banking deposit levels.

The Bank calculates the Herfindahl-Hirschman Index (HHI) on client deposit concentration by client group. Client Group is used rather than individual accounts as the risk is more properly assigned to the controlling entity. As the Bank serves commercial, corporate, and high-net worth clients it is common for a controlling entity to have control over multiple legal entities and accounts.

The Herfindahl-Hirschman Index (HHI) is a simple approach for quantifying undiversified idiosyncratic risk. The HHI is defined as the sum of the squares of the relative portfolio shares of all groups. Well-diversified portfolios with a very large number of very small entities have an HHI value close to zero whereas heavily concentrated portfolios can have a considerably higher HHI value. In the extreme case of a single entity, the HHI takes the value of one.

BCB uses both the raw Herfindahl Index (HI) and its reciprocal. The formula is;

HI:
$$H = \sum_{i=1}^N s_i^2$$

Reciprocal:
$$H_r = 1/H$$

The calculation is run against the aggregate balances of client groups (where a client controls multiple accounts) or individual clients that do not hold more than one account.

The following table explains how the HHI score is related to concentration and is derived from generally accepted definitions of concentration;

H is below 0.01 indicates a highly unconcentrated index.
H is below 0.1 indicates an unconcentrated index.
H is between 0.1 to 0.18 indicates moderate concentration.
H is above 0.18 indicates high concentration

As of this writing, the HHI for BCB's client portfolio is;

Herfindahl-Hirschman Index (HHI):	0.048
Equivalent Number of Groups:	20
Equivalent Balance Amount:	\$302,313,717
Percentage of Total Balances:	72.24%

A HHI score of 0.048 indicates that BCB's client concentration risk is 'unconcentrated', but not 'highly unconcentrated'. However in practice this level tends to result in a 'lumpy' dispersion of balances with resulting volatility in balance levels.

Compliance Risk

Like all banks BCB is a regulated entity that is supervised by the Bermuda Monetary Authority (BMA). The activity of the bank is subject to limits imposed through regulations and through legislation. The Bank must comply with these regulations and legislation or face sanction, fines, loss of license or restrictions on operations.

BCB is also indirectly impacted by the regulatory regimes of other countries with which it transacts business and to a degree is obligated to comply with those regulations. For example while BCB has no operations in the US it does use US banks for its deposits, US dollar clearing, etc. As such the US counterparty banks make requirements of BCB, such as completion of Patriot Act forms, compliance with periodic reviews, and compliance with US prohibition of transactions with entities sanctioned by the US (known terrorists and other Specially Designated Nationals or SDN list).

BCB actively manages compliance risk through a dedicated Compliance Manager who ensures that all business transacted by the bank meets domestic requirements, internal policy, and international requirements. The Compliance Manager monitors changes in legislation and updates bank policy and operations as needed. The Bank maintains compliance through a number of programs that includes;

- Real-time automated scrubbing of all wire transactions against official watch lists to detect potential activity with known sanctioned entities
- Review of all new business for risk and approval as well as continuous periodic review of all existing business on a risk-basis for compliance with regulations
- Activity monitoring using automated systems to detect patterns of suspicious activity (currently in test mode, live date estimated to be Q1 2010)
- Periodic training and update for all staff for anti-money laundering, anti-fraud, and internal policy & procedure

The Compliance function reports to the Chief Operating Officer and submits quarterly reports to the Board of Directors.

Additionally the Bank is subject to supervisory review and on-site inspection from the BMA, and elements of the compliance function are subject to audit by both the Banks internal auditor and its external auditor.

Operational Risk

Operational risk is deemed as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external causes, whether deliberate, accidental or natural.” Operational risk by its nature cannot be entirely eliminated but it can be managed and mitigated to levels that are deemed acceptable by management.

Operational risk is the responsibility of the Risk Committee and includes business process controls, data systems, and compliance (anti-money laundering). The Committee meets at least quarterly or more frequently as needed to review controls, incidents, and work underway to manage risk. Incident management team meetings are held as and when needed.

The Bank has traditionally used a probability matrix approach to evaluate potential operational risk events and set priorities. This approach is under review.

Core elements of an operational risk mitigation program for a bank include data security, process and control audits, and staff training.

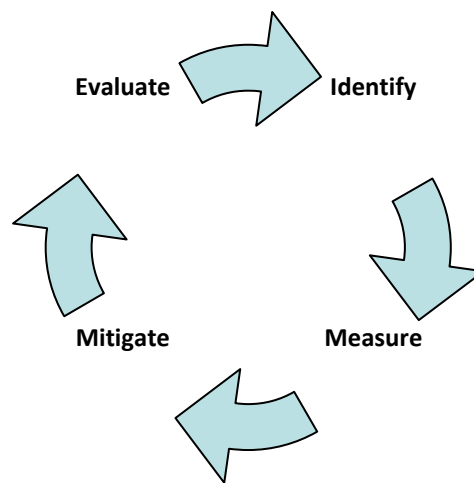
The Bank’s control environment includes non-automated risk management such as a program of continuous audit review and risk-based in depth client review. A series of daily reporting is delivered electronically to senior and executive management to ensure that the team is informed and take action if needed on operational and financial status.

The Bank also utilizes automated systems to mitigate risk associated with criminal activity through the Bank’s products and services. These systems include application risk scoring systems for new business uptake, real-time wire activity scrubbing against official watch-lists, the Banks automated activity monitoring systems will be fully operational during Q1 2010.

The key operational risk for banks tends to be fraud (internal or external), errors, and problems related to data systems. Compliance risk is a rapidly rising area of concerns for banks. Historically BCB has had little cost or losses from failed data systems or errors, and in recent years costs associated with fraud have been less than 0.2% of total capital.

Operational Risk Assessment

The fundamental process of assessing operational risk relies on the identification and measurement of risks, the mitigation of risks, and an evaluation of the efficacy of the mitigation. These risks can be inherent in a process, represent vulnerabilities, or manifest themselves through actual incidents.



The steps in the process are;

- Identify the risk: this means to identify a specific risk element, its probability and scope
- Measure the risk: determine the impact or exposure in terms of cost, and determine how this risk will be reported.
- Mitigate the risk: based on the cost of an incident take reasonable steps to manage the risk exposure.
- Evaluate the program: evaluate the mitigation work and determine if further work is required.

The risk event is evaluated in terms of probability and severity. It is tied to a reporting code that is used by the internal web-based reporting tool, and the adequacy of the controls is evaluated.

The impact types for a potential operational risk event are;

- Reputation risk
- Strategic risk
- Market risk
- Credit risk
- Legal & Compliance risk
- Liquidity risk

As noted above the potential risk events are linked via codes to an internal web-based reporting tool that captures the details of incidents. These reports are used to assign mitigation work, track the progress of responses to incidents and to feed into the Risk Management Committee.

Data Security

Banks by their nature are heavily data-dependant and the requirements for protecting the confidentiality, integrity, and availability of data are critical.

BCB has a multi-layered approach to data security and to date there have been no known systems breach of data integrity. Access controls are managed by the onsite technical department by a certified 'White Hat' specialist.

BCB does not outsource its technical operations and data remains in Bermuda.

Logical access control is in place at the individual application level as well as at the network level. Password complexity and mandatory changes are enforced programmatically. User profiles limit what a user can access, see or change. Application database systems are also locked down and strictly controlled.

Network assets are protected through the use of a DMZ architecture with firewalls at the external boundary and internally. Automated Intrusion Prevention Systems (IPS) operate in-line at the perimeter to monitor all Internet traffic for malicious code or attacks and drop the connections accordingly. Intrusion Detection Systems (IDS) are installed on the DMZ's, they monitors and report network activity for any anomalies.

Anti-virus software protects all desktop machines and servers, and where applicable application and systems updates and patches are applied automatically. Otherwise all updates go through a test lab to ensure compatibility with the Banks operating environment.

BCB has implemented PC Desktop End Point Security that centrally disables access to any portable device, guarding against data theft and the introduction of data or software that could be harmful to the network. Devices that are blocked include Floppy disks, CDs and DVD ROMs, iPods, Storage devices, Printers, PDAs, Network adapters, Modems, Imaging devices, and more.

The Bank maintains a 'hot' business recovery architecture with a fail-over time of a few minutes. The backup site readiness is monitored continuously and tested at least annually. The recovery site is in Bermuda and is considered by the Bank as a practical commercially reasonable approach.

BCB has implemented Web and email appliances to prevent accidental disclosure of bank data by applying granular, content-aware policies for both the Web and e-mail gateways from one centralized policy management console.

Internal Audit

The Bank has an Internal Audit department whose function is to review and test operational controls and work with management to improve or correct the control environment. The internal audit function reports to the Chief Operating Officer and to the Audit Committee of the Board.

The internal audit function is also a member or permanent guest of the various committees to provide guidance and to ensure that programs fit the control environment.

The Compliance Manager also performs checks on procedures to ensure compliance with Bank policy.

Human Resources

Our staff are an integral part of the control and risk mitigation environment. Through their direct contact with clients they build relationships that not only support excellent service but facilitate knowledge of the client's business and patterns of activity. Such a program supports low-error rate transaction handling, fraud detection, and suspicious activity detection.

All banks are from time to time subjected to attack from criminals and losses can happen. A fully informed and trained staff is a major control to mitigate this risk. BCB provides regular periodic training to all staff on anti-money laundering (it is also a regulatory requirement for a minimum of annual training for anti-money laundering), anti-fraud, and internal procedures. This training is mandatory for all staff at all levels.

Basel II

Bermuda has implemented the Basel II framework for capital assessment, of which this disclosure forms a part. Bermuda Commercial Bank has adopted the Basic Indicator Approach as being most appropriate for the scale and scope of the Bank's operations. Accordingly the Bank has agreed its Capital Adequacy and Risk Profile (CARP) document with the Bermuda Monetary Authority and currently operates with a minimum Capital Adequacy Ratio requirement of 19%.

The Bank's Capital Adequacy Ratio at September 30, 2009 was 29.35%.

Table of Key Figures as at September 30, 2009

Tier 1 Capital	\$73.0 million
Client liabilities (deposits)	\$345.5 million
Assets under Custody and Trust	\$420 million
Credit Exposure	\$0
FX Exposure	\$0
Commodities held	\$0
Securities held	\$12.9 million
Minimal regulatory capital adequacy ratio	19.0%
Actual regulatory capital adequacy ratio	29.36%