



REPUTATIONAL RISK MANAGEMENT MODULE

CONSULTATION

MODULE	RR Reputational Risk Management
	Table of Contents

		Date Last Changed
RR-A	Introduction	
	RR-A.1 Purpose	04/2018
	RR-A.2 Module History	04/2018
RR-1	Reputational Risk	
	RR-1.1 Introduction and Scope	04/2018
RR-2	Sources of Reputational Risk	
	RR-2.1 Key Drivers	04/2018
RR-3	Reputational Risk Management	
	RR-3.1 Reputational Risk Management Framework	04/2018
	RR-3.2 Assessment of Reputational Risk	04/2018
	RR-3.3 Management of Step-in Risk	04/2018

MODULE	RR: Reputational Risk Management
CHAPTER	RR-A: Introduction

RR-A.1 Purpose

Executive Summary

RR-A.1.1 The Reputational Risk Management Module sets out the Central Bank of Bahrain's ("CBB's") rules and guidance to conventional bank licensees operating in Bahrain on establishing parameters and control procedures to monitor and mitigate reputational risks. The content of this Module applies to all conventional bank licensees, except where noted in individual Chapters.

RR-A.1.2 This Module should be read in conjunction with other parts of the Rulebook, mainly:

- (a) Principles of Business;
- (b) High-level Controls;
- (c) Credit Risk;
- (d) Market Risk;
- (e) Operational Risk;
- (f) Liquidity Risk;
- (g) Interest Rate Risk in the Banking Book ("IRRBB");
- (h) Internal Capital Adequacy Assessment Process ("ICAAP"); and
- (i) Stress Testing.

Legal Basis

RR-A.1.3 This Module contains the CBB's Directive (as amended from time-to-time) relating to reputational risk management and is issued under the powers available to the CBB under Article 38 of the Central Bank of Bahrain and Financial Institutions Law 2006 ("CBB Law"). The Directive in this Module is applicable to all conventional bank licensees (including their approved persons).

RR-A.1.4 For an explanation of the CBB's rule-making powers and different regulatory instruments, see Section UG-1.1.

MODULE	RR: Reputational Risk Management
CHAPTER	RR-A: Introduction

RR-A.2 Module History

Evolution of the Module

RR-A.2.1 This Module was first issued in April 2018 as part of Volume One of the CBB Rulebook. All directives in this Module have been effective since this date. Any material changes that have subsequently been made to this Module are annotated with the calendar quarter date in which the change was made. Chapter UG-3 provides further details on Rulebook maintenance and version control.

RR-A.2.2 The most recent changes made to this Module are detailed in the table below:

Summary of Changes

Module Ref.	Change Date	Description of Changes

MODULE	RR: Reputational Risk Management
CHAPTER	RR-1: Reputational Risk

RR-1.1 Introduction and Scope

- RR-1.1.1 This Chapter provides CBB's requirements and guidance with respect to an effective reputational risk management and sets out the approach for banks to manage reputational risk.
- RR-1.1.2 Reputational risk can be defined as the risk arising from negative perception on the part of customers, counterparties, shareholders, investors, debt-holders, market analysts, other relevant parties or regulators that can adversely affect a bank's ability to maintain existing, or establish new, business relationships and continued access to sources of funding (e.g. through the interbank or securitisation markets). Reputational risk is multidimensional and reflects the perception of other market participants. Furthermore, it exists throughout the organisation and exposure to reputational risk is essentially a function of the adequacy of the bank's internal risk management processes, as well as the manner and efficiency with which management responds to external influences on bank-related transactions.
- RR-1.1.3 Reputational risk also may affect a bank's liabilities, since market confidence and a bank's ability to fund its business are closely related to its reputation. For instance, to avoid damaging its reputation, a bank may call its liabilities even though this might negatively affect its liquidity profile. This is particularly true for liabilities that are components of regulatory capital, such as hybrid/subordinated debt. In such cases, a bank's capital position is likely to suffer.
- RR-1.1.4 Once a bank identifies potential exposures arising from reputational concerns, it should measure the amount of support it might have to provide (including implicit support of securitisations) or losses it might experience under adverse market conditions. In particular, in order to avoid reputational damages and to maintain market confidence, a bank should develop methodologies to measure as precisely as possible the effect of reputational risk in terms of other risk types (e.g. credit, liquidity, market or operational risk) to which it may be exposed. This could be accomplished by including reputational risk scenarios in regular stress tests. For instance, non contractual off-balance sheet exposures could be included in the stress tests to determine the effect on a bank's credit, market and liquidity risk profiles. Methodologies also could include comparing the actual amount of exposure carried on the balance sheet versus the maximum exposure amount held off-balance sheet, that is, the potential amount to which the bank could be exposed.
- RR-1.1.5 A bank should pay particular attention to the effects of reputational risk on its overall liquidity position, taking into account both possible increases in the asset side of the balance sheet and possible restrictions on funding, should the loss of reputation result in various counterparties' loss of confidence. (See Liquidity Risk Management Module.)

RR-1.1 Introduction and Scope

RR-1.1.6

Banks must establish an effective process for managing reputational risk that is appropriate for the size and complexity of its operations.

RR-1.1.7

This Module focuses mainly on:

- (a) The approach to identifying and managing reputational risk;
- (b) Drawing attention to various sources of reputational risk;
- (c) Providing guidance on the key elements of reputational risk management; and
- (d) Promoting adoption of a formalized and structured approach to managing reputational risk.

MODULE	RR: Reputational Risk Management
CHAPTER	RR-2: Sources of Reputational Risk

RR-2.1 Key Drivers

RR-2.1.1 It is vital for banks to understand how different sources of reputational risk can impact their business operations, to set up appropriate systems and controls which can be used to manage these risks. It should be noted that many of the reputational drivers are inter-related, representing common factors applicable to banks, and relate to how well a bank has managed its business and controlled its material risks.

RR-2.1.2 The key drivers of reputational risk that could assist banks in identifying and categorising the major sources of reputational risk applicable to them, amongst others, are outlined below:

- (a) Corporate governance – good corporate governance is vital to a bank's reputation. The leadership of the Board and senior management will directly affect stakeholders' perception of the bank;
- (b) Board and management integrity – the personal ethics and behaviour of directors and senior management are important determinants of stakeholder confidence;
- (c) Staff competence/support – staff competence and support is essential for business success. Any deficiencies in employment and staff management practices could lead to various problems, which include high staff turnover, insufficient staffing, poor service quality, staff incompetence/misconduct, customer complaints and employee disputes. Some of these issues may result in damaging headlines and adverse publicity;
- (d) Corporate culture – it is crucial for banks to promote a corporate culture where the adoption of ethical and responsible behaviour, that can protect and enhance their reputation, is encouraged. Inadequate corporate culture may result in a loss of confidence;
- (e) Risk management and control environment – a sound risk management and control environment is essential for banks to safeguard their assets and capital, and to mitigate reputational risk. Banks should seek independent assurance that existing risk management and control systems are appropriate via internal audits, and take remedial actions for any deterioration in risk management and control standards;
- (f) Financial soundness/business viability – a bank's reputation is likely to suffer if its financial soundness, or business viability, is questioned. To safeguard and strengthen their reputation, banks should build-up stakeholder trust in their financial reporting systems, manage stakeholder expectations by providing relevant factual information to facilitate their assessment of the banks' financial performance and future prospects;
- (g) Business conduct and practices – banks are required to run their businesses in a responsible, honest and prudent manner. Business practices which deviate from this basic standard could erode stakeholder confidence and damage their reputation, and any resultant breach of laws and regulations may lead to investigations, disciplinary action and criminal charges. In dealing with customers and other counterparties, banks should be guided by, and adhere to, all relevant ethical standards and codes of conduct;

MODULE	RR: Reputational Risk Management
CHAPTER	RR-2: Sources of Reputational Risk

RR-2.1 Key Drivers (Continued)

- (h) Stakeholder satisfaction – a banks’ ability to satisfy stakeholder needs and expectations on a continuing basis is of utmost importance in sustaining their business in a highly competitive banking environment. Failure to do so, may result in loss of stakeholder confidence, falling business, adverse publicity or, in some cases, legal sanctions;
- (i) Legal/regulatory compliance – banks should adequately appraise legal and regulatory risks, and put in place robust systems to ensure compliance, including enhancing staff awareness of compliance issues and identifying areas of potential threat and vulnerability. Breaching the law or any relevant regulatory standards and guidelines can lead to serious consequences, including regulatory investigations, costly and high profile litigation, public censure, civil and criminal sanctions, harmful publicity, claims for damages, or even the loss of authorization. There may be significant damage to a bank’s reputation even if the bank is ultimately acquitted of any illegal conduct;
- (j) Contagion risk/rumours – banks operating as part of a group will be susceptible to reputational events affecting their parent bank, non-bank holding company, or other members of the group (e.g. subsidiaries and affiliates). Such contagion effects on a banks’ reputation may also result from other problematic relationships, such as any close association with major customers, counterparties or service providers that are revealed to be engaged in unethical, unlawful or corrupt activities. Rumours may have a damaging impact on the bank’s reputation and the level of public confidence. Therefore, adequate contingency procedures should be developed by banks;
- (k) Crisis management – a bank’s inadequate response to a crisis, or even a minor incident, that attracts media attention could arouse stakeholder concerns about management competence, thereby jeopardising the bank’s reputation. On the other hand, effective crisis management arrangements (including communications with stakeholders and the media) could quickly allay stakeholder fears, restore their confidence and even enhance reputation. Therefore, banks should ensure that they are ready to deal with possible crises (which may be unprecedented and totally unexpected), with detailed and well-rehearsed crisis management plans in place. Close attention should also be paid to managing media communications;
- (l) Transparency/accountability – a banks’ ability to be responsive to and satisfy stakeholders’ information needs (e.g. by disclosing information in respect of material issues of interest to stakeholders in a transparent, honest and prompt manner) has become a key determinant of business competence. Such information will help stakeholders in understanding a banks’ values, strategies, performance and future prospects. Stakeholder confidence, as well as the banks’ credibility and reputation, will be weakened if information disclosed is found to be misleading, inaccurate or incomplete. There should be adequate accountability for the integrity of information disclosures, which should be backed by robust management monitoring and reporting systems;

MODULE	RR: Reputational Risk Management
CHAPTER	RR-2: Sources of Reputational Risk

RR-2.1 Key Drivers (Continued)

- (m) Branding and cross-selling - this refers to the potential harm to a bank's reputation when an entity has clients in common with the bank and also carries the bank's brand (e.g. corporate name, logo/symbol). Different brand strategies create different risk profiles. Banks should consider the degree to which cross-selling is part of their overall strategy, as a greater degree of cross-selling increases reputational risk. This is particularly the case if a bank or banking group has stand-alone deposit-taking institution(s), broker-dealer(s) and asset management unit(s) that cross-sell products;
- (n) Outsourcing – a bank's reputation could also be damaged by sub-standard service quality, improper acts, or lax controls of some key service providers (e.g. outsourced telephone banking operations, IT support, debt collection services etc.). Banks should closely monitor the performance of the outsourcing providers and the on-going impact of the agreement on their risk profile, systems and controls framework; and
- (o) Shari'a non-compliance risk – Shari'a non-compliance is a unique operational risk in Islamic finance products resulting from non-compliance of the bank with the rules and principles of Shari'a in its products and services. It is crucial to set up key risk indicators for identifying the Shari'a non-compliance risk inherent in different kinds of Shari'a-compliant contracts, and to outline a set of variables that help to estimate the likelihood and severity of Shari'a non-compliance risk. It is possible for banks to become insolvent because of the reputational risk that is triggered by the Shari'a non-compliance risk. It is important to consider Shari'a non-compliance risk as one of the main risks that banks should take into account as part of their enterprise-level risk evaluation. Banks should be aware of the implications of Shari'a non-compliance risk for the overall enterprise when Shari'a requirements and rulings are not effectively communicated, translated into internal policy, or observed by banks across different businesses and functional units; and
- (p) Step-in risk – refers to the level of risk that is associated with a bank's decision to provide financial support to an unconsolidated entity that is facing stress, in the absence of, or in excess of, any contractual obligations to provide such support. The main reason for step-in risk is to avoid the reputational risk that a bank might suffer if it did not support an entity facing a stress situation. The financial crisis provided evidence that a bank might have incentives beyond contractual obligation or equity ties to 'step in' to support unconsolidated entities to which it is connected (refer to Section RR-3.4).

MODULE	RR: Reputational Risk Management
CHAPTER	RR-3: Reputational Risk Management

RR-3.1 Reputational Risk Management Framework

RR-3.1.1

Banks must adopt an approach to reputational risk management that fits the banks' profile of activities and level of sophistication, and that enables the risks affecting reputation to be consistently and comprehensively identified, assessed, controlled, monitored and reported.

RR-3.1.2

The key elements of reputational risk management are good corporate governance, the existence of highly skilled, sincere and honest resources, effective reputational risk management processes; and adequate management of reputational events.

Good Corporate Governance

RR-3.1.3

Good corporate governance forms the foundation of effective reputational risk management and provides a framework for:

- (a) Guiding banks' conduct and actions in achieving their vision, values, goals and strategies, as well as meeting stakeholder requirements and expectations; and
- (b) Ensuring robust oversight of their conduct and actions.

RR-3.1.4

Good corporate governance can be achieved by implementing a governance infrastructure and adopting governance practices in compliance with Module HC (High-level Controls).

RR-3.1.5

The Board must be responsible for overseeing the overall reputational risk management processes.

RR-3.1.6

A sound governance infrastructure should have the following general attributes:

- (a) Having the right people, with the right balance of skills and experience on the Board, with suitable checks in place to ensure that no single individual can influence Board decisions;
- (b) Including a robust framework for succession planning to ensure that the business can continue to function effectively, even when there is a major management or staff turnover; and
- (c) Enabling business and management performance to be closely overseen by independent directors.

RR-3.1.7

Banks should adopt a governance approach that sets out clear governance objectives and expectations on reputational risk management, as well as the authorities and responsibilities of all parties engaged in the risk management process.

MODULE	RR: Reputational Risk Management
CHAPTER	RR-3: Reputational Risk Management

RR-3.1 Reputational Risk Management Framework (Continued)

RR-3.1.8

The following elements must be included in the banks' governance practice framework:

- (a) Setting a clear and unambiguous vision, values, goals and strategies, and ensuring that they are transparent;
- (b) Developing appropriate policy, codes of conduct, guidelines and procedures to support the implementation of the bank's vision, values, goals and strategies;
- (c) Creating an open and empowering corporate culture to encourage responsible and ethical behaviour, and to support the achievement of business objectives and effective risk management;
- (d) Building up a strong, stable management team that are honest, competent, responsible, accountable and responsive to stakeholders;
- (e) Raising the risk awareness of employees and providing employees with adequate training;
- (f) Setting up effective systems and controls to manage and control all material risks (including reputational risks) faced by the bank and to monitor compliance with all applicable laws, regulatory standards, best practices and internal guidelines; and
- (g) Having adequate policy and procedures in place to ensure that all disclosures to stakeholders are clear, accurate, complete, relevant, consistent and timely, and guided by the principles of ethics, integrity and transparency.

Effective Reputational Risk Management Process

RR-3.1.9

Banks must have adequate arrangements, strategies, policy, processes and mechanisms in place to manage reputational risk. An effective reputational risk management process must include:

- (a) Policy, definition of roles, codes of conduct, guidelines and procedures which guide staff behaviour and conduct, and set boundaries for staff actions, in particular the boundaries for unacceptable practices;
- (b) Consideration of the potential impact of its strategy and business plans and, more generally, of its behaviour on its reputation;
- (c) Addressing reputational risk in a precautionary manner, for example by setting limits or requiring approval for allocating capital to specific countries, sectors or persons and/or whether its contingency plans address the need to deal proactively with reputational issues in the event of a crisis;

MODULE	RR: Reputational Risk Management
CHAPTER	RR-3: Reputational Risk Management

RR-3.1 Reputational Risk Management Framework (Continued)

- (d) Risk identification, assessment and control which provides a systematic process for identifying and assessing the risks affecting reputation, including the setting of appropriate response actions to control the risks;
- (e) Risk monitoring and reporting which ensures that the progress of carrying out agreed response plans is adequately monitored, any changes to the status of the risks concerned is regularly reviewed, and early warning systems are in place for identifying emerging threats, to ensure that prompt corrective actions are taken to address those threats;
- (f) Communications and disclosures which enable meaningful, transparent and timely information to be provided to stakeholders to better their understanding of the bank's performance and future prospects, and to retain their confidence; and
- (g) Independent reviews and audits which give assurance that the risks affecting reputation have been adequately understood and properly controlled throughout the bank.

Adequate Management of Reputational Events

RR-3.1.10

Reputational events may still occur despite stringent risk control measures. As such, banks must develop a systematic and comprehensive approach for managing reputational events. This will allow bank management to be prepared to take proper measures to restore the institution's reputation and minimize any damage caused. The effectiveness of this approach would help reduce the chance of having to deal with a full-blown crisis.

RR-3.1.11

The bank's approach to manage reputational events must include:

- (a) Crisis management adoption of the key elements of effective crisis management, which includes a crisis management manual, crisis management structure, invocation of crisis management, crisis management process, internal and external communications, and pre-planning for crisis management;
- (b) Adoption of an embedded risk mitigation approach that refers to shaping products, business transactions, special investments, outsourcing arrangements, new product process, restructurings etc., which will assist in mitigating some of the potential concerns of key stakeholders by design;

MODULE	RR: Reputational Risk Management
CHAPTER	RR-3: Reputational Risk Management

RR-3.1 Reputational Risk Management Framework (Continued)

- (c) Post-event reviews – the Board and senior management must conduct a post-event review to identify any lessons learnt, or problems and weaknesses revealed, from the event in order to take appropriate actions to improve the bank’s approach for managing reputational risk; and
- (d) Early warning systems – a banks’ implementation of early warning systems will enable them to plan actions in advance for addressing potential threats that are likely to develop into reputational events. Early recognition of impending reputational problems also means that valuable time has been won to facilitate pre-planning for future action.

RR-3.1.12

The early warning systems must also involve developing and monitoring:

- (a) Performance indicators and other indicators reflecting stakeholder confidence, which can provide an estimate of the bank’s reputation and keep track of the progress in managing associated risks; and
- (b) Early warning indicators (e.g. a sudden increase in customer complaints, breaches of internal controls, operational errors, system outages, fraudulent incidents and any significant deterioration in other performance indicators) and other triggers or thresholds for management actions, or provide signals to invoke response or contingency plans.

MODULE	RR: Reputational Risk Management
CHAPTER	RR-3: Reputational Risk Management

RR-3.2 Assessment of Reputational Risk

RR-3.2.1

Banks must conduct a regular assessment of the reputational risk to which they are exposed, leveraging their understanding of governance, business model, products and the environment in which they operate.

RR-3.2.2

Banks must consider both internal and external factors or events that might give rise to reputational concerns (refer to Section RR-2.1). Banks must consider the following qualitative indicators, amongst others, in their assessment of reputational risk:

- (a) The number of sanctions from official bodies during the year;
- (b) Media campaigns and consumer-association initiatives that contribute to a deterioration in the public perception and reputation of the institution;
- (c) The number of and changes in customer complaints;
- (d) Malpractices and irregularities;
- (e) Negative events affecting the institution's peers;
- (f) Dealing with sectors that are not well perceived by the public (e.g. weapons industry, embargoed countries etc.) or people and countries on sanctions lists; and
- (g) Other 'market' indicators, for example, rating downgrades or changes in the share price throughout the year.

RR-3.2.3

Banks must assess the significance of its reputational risk and how it is connected with other risks (i.e. credit, market, operational, liquidity and interest rate risks) by leveraging other risk assessments to identify any possible secondary effects in either direction (from reputation to other risks and vice versa).

MODULE	RR: Reputational Risk Management
CHAPTER	RR-3: Reputational Risk Management

RR-3.2 Assessment of Reputational Risk (Continued)

Stress Testing

RR-3.2.4

Banks must enhance their stress testing methodologies to capture the effect of reputational risk. Banks must also conduct stress testing or scenario analysis to assess any secondary effects of reputational risk (e.g. liquidity, funding costs, etc.).

RR-3.2.5

The stress testing technique is useful for identifying events or changes that pose threats to banks, and can help develop different sets of circumstances which could potentially cause a crisis. Banks can make use of this technique to assess the likelihood of the risk materialising and the potential impact of the risk on their business and reputation under different stress scenarios (refer to Module ST on Stress Testing for guidance).

RR-3.2.6

Banks should be guided by the following supplementary guidance on use of stress testing for reputational risk:

- (a) Banks employing stress testing techniques for assessing reputational risk should seek to incorporate stress scenarios for reputational risk into their institution-wide stress testing procedures and assess the impact of reputational risk on other major risks (e.g. business or liquidity risk);
- (b) In developing stress scenarios for reputational risk, banks should identify the major sources of reputational risk to which they are potentially exposed, key stakeholders that will most likely increase reputational risks in stress scenarios or an appropriate range of circumstances and events. Banks should also consider how those sources, circumstances and events may adversely affect their business prospects and financial position (including earnings, capital and liquidity), as well as generate other second round effects;
- (c) Banks may face reputational risk in other aspects, such as those arising from material weaknesses in their internal risk management processes (e.g. resulting in substantial fraudulent losses) or management's failure to respond swiftly and effectively to external threats or influences (e.g. resulting in poor strategic decisions). Banks should exercise their best judgment and apply stress scenarios and parameters that suit their own circumstances and risk profile;

MODULE	RR: Reputational Risk Management
CHAPTER	RR-3: Reputational Risk Management

RR-3.2 Assessment of Reputational Risk (Continued)

- (d) Once the potential exposures arising from reputational concerns are identified, banks should estimate the amount of support (capital or liquidity) they may have to provide, as well as estimate potential loss under adverse market conditions. Banks should also assess the impact of reputational risk on other risks to which they may be exposed. This could be accomplished by including reputational risk scenarios in regular stress tests;
- (e) Banks should assess whether there is any longer term impact on their business and operations due to reputational risk (e.g. loss of market share, customer base or business revenue). Banks should also pay particular attention to the effects of reputational risk on their overall liquidity position, taking into account both possible changes in the asset side of the balance sheet and possible restrictions on funding, should the damage in reputation result in a general loss of confidence on the part of their counterparties and customers; and
- (f) Senior management should actively participate in conducting stress testing and scenario analyses for reputational risk (including the development of stress scenarios and assumptions), and review the stress testing results.

MODULE	RR: Reputational Risk Management
CHAPTER	RR-3: Reputational Risk Management

RR-3.4 Management of Step-in Risk

Banks' Policy and Procedures for Identifying and Managing Step-in Risk

RR- 3.4.1

Banks must establish and maintain, as part of their risk management framework, policy and procedures that describe the processes used to identify entities that are unconsolidated for regulatory purposes and the associated step-in risks. The policy and procedures must:

- (a) Clearly describe the identification criteria that banks use to identify the step-in risk;
- (b) Not be prescriptive or geared towards any particular type of entity. Given the case-by-case nature of the evaluation, the guidelines are envisaged as flexible enough to capture all entities that are unconsolidated for regulatory purposes and which pose significant step-in risk;
- (c) Clearly describe the specific provisions of the laws or regulations and list the types of entity covered by those laws or regulations;
- (d) Describe the internal function responsible for identifying, monitoring, assessing, mitigating and managing the potential step-in risk;
- (e) Clearly describe the bank's own definition and criteria of 'materiality', as used to exclude immaterial entities in the bank's step-in risk assessment, and their rationale;
- (f) Document the process to obtain the necessary information to conduct the regular self-assessments;
- (g) Be reviewed regularly, and whenever there is any material change in the types of entity or in the risk profile of entities; and
- (h) Require the 'Step-in Risk Self-assessment' to be included in the internal risk management processes, subject to independent controls.

MODULE	RR: Reputational Risk Management
CHAPTER	RR-3: Reputational Risk Management

RR-3.4 Management of Step-in Risk (Continued)

Regular Step-in Risk Identification and Assessment

RR- 3.4.2

Banks must regularly identify all entities giving rise to step-in risk. For all these entities, they must estimate the potential impact on their liquidity and capital that step-in risk could entail. The bank must use the estimation method it believes to be most appropriate. Banks must describe the method used to estimate the financial impact of step-in risk in each case.

Step-in Risk Reporting

RR- 3.4.3

Banks must annually report the results of their self-assessment of step-in risk to the CBB on 30th April of each year. The report must contain the following information:

- (a) Per groups of similar entities, the number and types of entity that were initially identified;
- (b) The entities must be grouped under three categories: entities deemed immaterial (for which no step-in risk assessment process conducted); entities which are material, but for which step-in risk is insignificant; and entities which are material and for which step-in risk is significant; and
- (c) The nature of the step-in risk and the action taken by the bank to limit, mitigate or recognise this risk, must be reported for entities which are material and for which step-in risk is significant.