Managing Reputational Risk

Mapping risk appetite against risk exposure

18 March 2019

Jennifer Hanley-Giersch
Managing Partner—Berlin Risk

Jennifer.hanley@berlinrisk.com
Table of Contents

1 Executive Summary .......................................................................................................................... 3
2 Introduction .................................................................................................................................... 4
3 Background ..................................................................................................................................... 5
   3.1 Definitions ................................................................................................................................. 6
   3.2 Regulatory Framework—Supervisory Guidelines and Recommendations ............................... 8
       3.2.1 Basel Committee on Banking Supervision ........................................................................ 8
       3.2.2 European Banking Authority ............................................................................................ 9
       3.2.3 Office of the Comptroller of the Currency ......................................................................... 10
       3.2.4 Office of the Superintendent of Financial Institutions ..................................................... 12
   3.3 Reputational Risk Assessment ................................................................................................. 13
   3.4 Industry practices ..................................................................................................................... 14
4 Solution .......................................................................................................................................... 16
   4.1 Introduction ............................................................................................................................... 16
   4.2 Methods and Approaches .......................................................................................................... 16
       4.2.1 Stakeholders Risk Assessment Methodology and Workflow ............................................ 16
       4.2.2 Reputational Risk Identification ....................................................................................... 18
       4.2.3 Reputational Risk Analysis .............................................................................................. 20
       4.2.4 Reputational Risk Evaluation ............................................................................................ 22
       4.2.5 Internal Controls—Reputational Risk in the Context of the AML Audit Risk Model .......... 23
5 Outlook ........................................................................................................................................... 24
6 Works Cited ..................................................................................................................................... 25
   6.1 Books and Articles ..................................................................................................................... 25
   6.2 Regulatory and Industry Guidance ............................................................................................ 25
1 Executive Summary

Numerous investigations resulting in costly legal proceedings have led to an increased and sustained erosion of public confidence in the financial sector in recent years, having a detrimental effect on the reputation of some of the world’s largest financial institutions. In total, some US$26 billion in fines have been imposed in anti-money laundering and sanctions violations globally in the last decade. Although the largest number of fines are seen in the US and in Europe, regulators in Asia and the Middle East are also taking a closer look at the regulatory frameworks of their financial institutions. The negative impact is lingering on, and some organisations are struggling to get back what once used to be a great reputation embedded in a perception of trust and confidence. Given this backdrop, reputational risk management has become an important strategic topic both from the perspective of the supervisors trying to ensure the stability of the financial system but also internally within financial institutions, which are under pressure to improve their anti-financial crime (AFC) frameworks and to regain trust with their customers and the wider public.

Based on research of a range of regulatory frameworks and supervisory guidelines, it is clear that the management board of any organisation should therefore ensure that senior management establishes a risk management system for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating reputational risk with foresight based on a sound methodological approach, which can be controlled and audited effectively. Anti-financial crime (AFC) programmes have an important role to play within this context.

A common approach to assessing reputational risk consists in comparing the expectations of the relevant stakeholders to the organisation’s activities, identifying potential gaps between expectations and performance, developing risk scenarios from those gaps, and assessing their likelihood and possible adverse effects on the organisation’s business model.

The paper sets out methods and approaches to managing reputational risk based on theoretical discussion and best-practice approaches, and offers general guidance for a reputational risk assessment workflow, using the Bow-Tie Technique, in order to provide a forward-looking view and in order to manage and monitor reputational risk effectively over time. This is based on a “causal approach” to reputational risk assessment, including components of risk identification, risk analysis, and risk evaluation.

The internal audit function (IAF) should verify and evaluate the quality and use of qualitative risk identification and assessment tools and the risk mitigation measures taken. In the case of reputational risk management, the IAF should ensure adequate identification; measurement and mitigation of reputational risks related to the AFC function; and compliance with laws, regulations, supervisory requirements, and the institution’s internal policies, processes, rules, and decisions.
2 Introduction

Numerous investigations resulting in costly legal proceedings have led to an increased and sustained erosion of public confidence in the financial sector in recent years. In total, some US$26 billion in fines have been imposed in anti-money laundering and sanctions violations globally in the last decade.\(^1\) HSBC Holdings Plc was fined a record US$1.92 billion in the US for money laundering. In 2016, Commerzbank paid some US$1.45 billion in penalties to settle sanctions and money laundering-related charges. In December 2018, Bank of America Merrill Lynch and Morgan Stanley were fined for sanctions violations. Deutsche Bank was fined US$258 million for sanctions violations.\(^2\) Some media reports state that Denmark's largest bank could be fined up to US$8 billion for money laundering in what marked Europe's largest scandal in 2018 involving numerous other financial institutions, including Deutsche Bank, as the investigation unfolds.\(^3\) Although the largest number of fines are seen in the US and in Europe, regulators in Asia and the Middle East are also taking a closer look at the regulatory frameworks of their financial institutions.

These cases have had a detrimental effect on the reputation of some of the world's largest financial institutions. The negative impact is lingering on, and some organisations are struggling to get back what once used to be a great reputation embedded in a perception of trust and confidence. Given this backdrop, reputational risk management has become an important strategic topic both from the perspective of the supervisors trying to ensure the stability of the financial system but also internally within financial institutions, which are under pressure to improve their anti-financial crime (AFC) frameworks and to regain trust with their customers and the wider public.

This paper looks at the landscape in which the discussions around reputational risk have evolved in recent years with a particular focus on the topic of anti-financial crime.

---

2. Other cases are mentioned here also: [https://www.acamstoday.org/kyc-enhanced-requirements/](https://www.acamstoday.org/kyc-enhanced-requirements/)
3 Background

The management board of any organisation should ensure that senior management establishes a risk management system for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating risks regularly. Reputational risk management is one of those risk areas and will form the key focus of this paper.

Reputational risk directly impacts an organisation’s strategy and is therefore one of the most important risks to manage with foresight based on a sound methodological approach, which can be controlled and audited effectively.

Reputational risk management frameworks and internal controls should assist in reducing reputational risk and its impact on an organisation. Anti-financial crime (AFC) programmes have an important role to play within this context given the high exposure organisations have to financial crime risk. The processes by which financial institutions detect, deter, and prevent financial crime and how they are embedded into the wider Enterprise Risk Management Framework is also key to the programme’s success and to its impact on the safety and soundness of national and international financial systems as a whole.

The following section will set the framework for discussion around this topic, starting with key definitions relevant to the issues presented in this paper.
### 3.1 Definitions

Following are key terms relevant to this white paper.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputational risk</td>
<td>Reputational risk is the risk to current or projected financial condition and resilience arising from negative public opinion. This risk may impair a bank’s competitiveness by affecting its ability to establish new relationships or services or continue servicing existing relationships. Reputational risk is inherent in all bank activities, and management should deal prudently with stakeholders, such as customers, counterparties, correspondents, investors, regulators, employees, and the community. A bank that actively associates its name with products and services offered through outsourced arrangements or asset management affiliates is more likely to have higher reputational risk exposure. Significant threats to a bank’s reputation also may result from negative publicity regarding matters such as unethical or deceptive business practices, violations of laws or regulations, high-profile litigation, or poor financial performance. The assessment of reputational risk should take into account the bank’s culture, the effectiveness of its problem-escalation processes and rapid-response plans, and its engagement with news media.⁴</td>
</tr>
<tr>
<td>Risk exposure</td>
<td>Based on the outcome of a risk assessment and the identification of its residual risk and including any trigger events, an organisation can define its risk exposure.⁵ So for example, following the release of the Panama Papers, any organisations with links to Mossack Fonseca &amp; Co. would have an increased risk exposure.</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>Risk appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity’s risk management philosophy, and in turn influences the entity’s culture and operating style. Risk appetite guides resource allocation. Risk appetite [assists the organization] in aligning the organization, people, and processes in [designing the] infrastructure necessary to effectively respond to and monitor risks. An organisation’s risk appetite is formalised in its Risk Appetite Statement.</td>
</tr>
<tr>
<td>Risk limits</td>
<td>Risk limits are linked to a firm’s Risk Appetite Statement allocated by risk types, business units, business lines, or product level. Risk limits are used by management to control the risk profile and linked to compensation programmes and assessment.⁷ A limit is essentially one or more numerical thresholds defined in relation with a specific risk exposure. Internal risk policy limits aim to contain risk exposures below an acceptable level.⁸</td>
</tr>
</tbody>
</table>

⁶ [https://www.coso.org/Pages/erm-integratedframework.aspx](https://www.coso.org/Pages/erm-integratedframework.aspx)
| Risk tolerance | The Institute of Risk Management defines risk tolerance as the boundaries of risk-taking outside of which the organisation is not prepared to venture in the pursuit of its long-term objectives. Risk tolerance can be limited by legal or regulatory requirements. |

---

9 [https://www.theirm.org/media/3779216/64355_Riskapp_A4_web.pdf](https://www.theirm.org/media/3779216/64355_Riskapp_A4_web.pdf)
3.2 Regulatory Framework—Supervisory Guidelines and Recommendations

The following sections provide an overview of those international organisations involved in setting best-practice regulatory standards within the banking sector as well outlining the requirements set out by the US, Canadian, and EU regulators with regard to reputational risk management. Within the scope of this white paper, we have not taken a global assessment of regulatory approaches or a differentiated approach on the country level drilling down into individual regulations as defined by individual EU member states. For the purpose of this white paper, research includes the approaches set out by the European Banking Authority (EBA), the Basel Committee on Banking Supervision, the US Office of the Comptroller of the Currency, and the Canadian Office of the Superintendent of Financial Institutions. The Monetary Authority of Singapore also appears to adopt a similar approach to the standards set out by the Basel Committee on Banking Supervision. The points relevant to reputational risk management from the perspective of this white paper are outlined in the following sections.

3.2.1 Basel Committee on Banking Supervision

The widely quoted definition of reputational risk as suggested by the Basel Committee on Banking Supervision in 2009 (Enhancements to the Basel II framework) offers a good starting point: “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.”

The Basel Committee also believes that most financial institutions’ key reputational asset is credibility, and underlines that “the concept of credibility thus captures the strategic perspective of reputational risk management, which essentially aims to maintain trust, confidence and support of the key stakeholders in order to enable the control and continuity over its mission and operations.”

In July 2009, the Basel Committee on Banking Supervision issued Enhancements to the Basel II framework, which included Pillar 2 (supervisory review process) guidance on reputational risk and implicit support. It noted (in paragraph 48), “Reputational risk can lead to the provision of implicit support, which may give rise to credit, liquidity, market and legal risk—all of which can have a negative impact on a bank’s earnings, liquidity and capital position. A bank should identify potential sources of reputational risk to which it is exposed. These include the bank’s business lines, liabilities, affiliated operations, off-balance sheet vehicles and the markets in which it operates. The risks that arise should be incorporated into the bank’s risk management processes and appropriately addressed in its ICAAP and liquidity contingency plans.” In its Guidelines—Identification and management of step-in risk, the Basel Committee noted that its position in this regard remains unchanged, highlighting at the same time that the implementation of such provisions remains a challenge for banks and for supervisors.

---

11 https://www.bis.org/publ/bcbs157.pdf
12 https://www.bis.org/publ/bcbs157.pdf
13 https://www.bis.org/publ/bcbs157.htm
14 https://www.bis.org/bcbs/publ/d423.pdf
Paragraph 54 of the Basel Committee’s Enhancement to the Basel II Framework notes, “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… 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.”

3.2.2 European Banking Authority

The EBA’s guidelines on internal controls note that institutions should have a holistic institution-wide risk management framework extending across all its business lines and internal units, including internal control functions, recognising fully the economic substance of all its risk exposures. The risk management framework should enable the institution to make fully informed decisions on risk-taking. The risk management framework should encompass on- and off-balance-sheet risks as well as actual risks and future risks to which the institution may be exposed. Risks should be evaluated from the bottom up and from the top down, within and across business lines, using consistent terminology and compatible methodologies throughout the institution and at consolidated or sub-consolidated levels. All relevant risks should be encompassed in the risk management framework with appropriate consideration of both financial and non-financial risks, including credit, market, liquidity, concentration, operational, IT, reputational, legal, conduct, compliance, and strategic risks.

The EBA guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) include reputational risk under operational risk, recognizing the strong links between the two. It also states that the outcome of reputational risk assessment should not be reflected in the scoring of operational risk but as part of the business model analysis and the liquidity risk assessment “since the main effects it can have are reductions in earnings and loss of confidence in/or disaffection with the institution by investors, depositors or interbank-market participants.” (paragraph 235)

The link between reputational risk and liquidity risk as a consequence is also significant given that funds are raised on the capital markets. While operational risk is indeed linked to reputational risk in many ways (see below), these links refer to the internal process dimension of reputational risk that is controllable to a large extent, and open to preventive measures. At the same time, however, reputational risks also have an external dimension that is outside an institution’s immediate control, such as customer conduct or the change in the political and economic environment in a country. The involvement of offshore-structure companies gives more cause for reputational concern than before, following the publication of the Panama Papers or the Paradise Papers, for example.

15 https://www.bis.org/publ/bcbs157.pdf
16 https://www.bis.org/publ/bcbs157.pdf
3.2.3 Office of the Comptroller of the Currency

According to the OCC’s Handbook on Corporate Risk Governance, a risk governance framework\(^{18}\) is an essential component in effectively managing the bank’s enterprise-wide risks. The framework is the means by which the board and management establish and reinforce the bank’s risk culture, articulate and monitor adherence to the risk appetite\(^ {19}\), and establish a risk management system with three lines of defence to identify, measure, monitor, and control risks. Reputational risk is listed among the other applicable risk categories (credit, interest rate, liquidity, price, operational, compliance, strategic). See the graphic that follows for a visualisation of a risk governance framework\(^ {20}\).

The board is responsible for overseeing the design and implementation of a risk governance framework. The board should require periodic independent assessments to determine the framework’s effectiveness, which may involve reviewing components of or the entire framework. Senior management is responsible for developing and maintaining the risk governance framework, which enables management to

\(^{18}\) A part of the corporate governance framework, through which the board and management establish and make decisions about the bank’s strategy and risk approach; articulate and monitor adherence to risk appetite and risk limits through the bank’s strategy; and identify, measure, monitor, and control risks

\(^{19}\) Risk appetite: Aggregate level and types of risk that a bank is willing to assume to achieve its strategic objectives and business plan. It is based on quantitative measures expressed relative to earnings, capital, risk measures, liquidity, and other relevant measures as appropriate. It also addresses reputation risk as well as money laundering and unethical practices.


effectively identify, measure, monitor, control, and report risk exposures consistent with the board-established risk appetite. Senior management should report to the board on the bank’s overall risk profile, including aggregate and emerging risks.

<table>
<thead>
<tr>
<th>Risk category</th>
<th>Quantity of risk</th>
<th>Quality of risk management</th>
<th>Aggregate level of risk</th>
<th>Direction of risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Low, moderate, high)</td>
<td>(Weak, insufficient, satisfactory, strong)</td>
<td>(Low, moderate, high)</td>
<td>(Increasing, stable, decreasing)</td>
</tr>
</tbody>
</table>

Operational

Compliance

Strategic

Reputation

The strength and level of transparency of a bank’s corporate and risk governance structure influence the bank’s reputation with shareholders, regulators, customers, other stakeholders, and the community at large. A responsible corporate culture and a sound risk culture are the foundation of an effective corporate and risk governance framework and help form a positive public perception of the bank. A bank that fails to implement effective corporate and risk governance principles and practices may hinder the bank’s competitiveness and adversely affect the bank’s ability to establish new relationships and services or to continue servicing existing relationships. Departures from effective corporate and risk governance principles and practices cast doubt on the integrity of the bank’s board and management. History shows that such departures can affect the entire financial services sector and the broader economy.

22 OCC Handbook: Corporate and Risk Governance, p.100
3.2.4 Office of the Superintendent of Financial Institutions

In 2005, the Canadian Office of the Superintendent of Financial Institutions (OSFI) noted that as financial institutions face a more global and complex marketplace, the importance and priority given to reputational risk management will continue to grow.\(^{23}\) Although the Canadian regulator noted at the time that reputational risk management was a growing area for regulators, it announced that it did not intend to establish specific guidance for the control and management of reputational risk. Nonetheless, OSFI did note that improving the effectiveness of reputational risk management practices should be a priority for all organisations.

With regard to the audit function, OSFI noted that financial institutions should ensure their practices for controlling reputational risk are periodically reviewed by internal audit (or through another independent assessment process), and that issues are addressed in a timely and on-going basis. OSFI noted the need for improved methodologies to better incorporate an assessment of reputational risk management practices into ongoing internal audit reviews.\(^{24}\) The regulator’s website, which was last modified in 2015, recognised that dealing with reputational risk is challenging, but it is an area that OSFI considers vital to ensuring that Canadian financial institutions continue to be managed in a safe and sound fashion. The announcement also noted that although OSFI recognises that “financial institutions have taken significant steps to manage reputational risk, more could be done”.\(^{25}\)

3.3 Reputational Risk Assessment

The strategic purpose of every risk assessment, in this case reputational risk assessment, is to prevent the risk event from occurring, or to use controls to reduce the likelihood of the risk event occurring; should the risk event occur anyway, be prepared by using mitigants to reduce the impact and/or the reputational damage. The latter involves the engagement with the stakeholders, whose actions essentially determine the level of reputational impact and damage. The very nature of reputational risk may provide opportunities, given that proactive risk management, including stakeholder engagement, offers the opportunity to build reputational capital with the stakeholders, which can be useful should a reputational risk event occur.

As noted by Elms and Low, “an even more complex system risk is reputational risk where “unacceptable behaviour”, such as the use of child labour, food contamination, or environmental abuses, in any stage of the supply chain may interact with increasing public attention to particular dimensions of performance and changes in the thresholds of what is deemed acceptable. Changes in any element can set off an escalating dynamic.” Elms and Low added that “it is important to note that while reputational risk is best understood as a consequence rather than a source of risk, it is the result of a complex set of system interactions”. As such, it is key to manage the sources of such risks rather than merely engage in damage control to reduce the consequences.  

In 2007, Eccles, Newquist, and Schatz stated in a Harvard Business Review article, Reputation and its Risks, that “reputation is a matter of perception” and that “the goal of any strategic effort to address reputation risk must necessarily identify the perception/reality gap and close it.” Andrea Bonime-Blanc developed this concept further, and stated that based on this, “any framework for identifying reputation risk must measure its perception among the organization’s stakeholders”.

Any reputational risk assessment methodology should include best-practice standards and refer to ISO 31000, in particular 5.4 Risk Assessment, and its components of risk identification, risk analysis, and risk evaluation. It should incorporate state-of-the-art risk assessment techniques, namely the Bow-Tie Technique (see also ISO/IEC 31010), which allows for an integrated, causal approach to assessing reputational risk. An explanation of this methodology follows, providing an overview of the general assessment process.

---

3.4 Industry Practices

The commercial bank Unicredit represents an example of a sophisticated risk assessment methodology that emerged from a review of the relevant literature. Unicredit acknowledges that reputational risk is not just a secondary risk emanating from primary operational risk within the bank, but should be assessed separately as emanating from external sources of risk, such as a customer’s characteristics and behaviour, particular countries and sectors of operation, and the nature of a project and transaction. Compliance issues, political issues, and issues related to environmental and social responsibility are therefore key in assessing the bank’s key vulnerabilities to reputational risk.

As for the analysis of reputational risk, Unicredit assesses the degree of exposure to a relevant risk cause combined with the probability that the manifestation of such risk causes, i.e. a risk event, might entail a reputational risk; the latter depends, for example, on the media coverage and publicity of the risk event. The second stage assesses the relevant stakeholders’ reaction by determining the level of attention combined with the intensity of the potential reaction to a risk event. Thus the severity analysis of reputational risk is eventually depicted in two dimensions, the probability of the reputational risk event combined with the expected intensity of the stakeholder reaction. Unicredit refrains from quantifying reputational risk and classifies it as low-, medium- and high-risk, which enables the representation of risk severity in a risk matrix and translates into a “traffic light” system.

Commerzbank, for example, seems to take a similar approach and states on its website that its Reputational Risk Management department uses a qualitative approach to reputational risk management and cooperates closely with other relevant units. Transactions and business relationships in which aspects of sustainability play a material role are extensively researched, analysed, and subjected to wide-ranging evaluation. At the extreme, this may lead to a rejection of a transaction or termination of a business relationship.

Some organisations emphasise the governance structure around reputational risk management as opposed to the methodology. HSBC’s website, for example, notes that governance of reputational risk management is integrated into the Group’s broader risk governance framework. There are currently three risk stewards for reputational risk: the Group Head of Communications, the Global Head of Financial Crime Compliance, and the Global Head of Regulatory Compliance. The Group Reputational Risk Committee, chaired by the Group chief risk officer, is the formal governance committee established to provide recommendations and advice to the Group’s senior management on reputational risk and customer selection matters that either present a serious potential reputational risk to HSBC or merit a Group-led decision. Formal governance committees exist at global, regional, and/or country levels across the Group’s global businesses to provide recommendations and advice on customers/transactions and non-customers (e.g. third parties) and wider reputational risks.

Deutsche Bank notes on its website that a reputational risk framework was installed in 2015, and explains the management structure around the topic highlighting aspects such as accountability and ownership.

Other organisations have increased their focus on reputational risk well beyond financial crime to include environmental, social, and governance (ESG) risks. ING’s Environmental and Social Risk Framework offers a good example.\(^\text{32}\)

4  Solution

4.1  Introduction

A common approach to assessing reputational risk consists of comparing the expectations of the relevant stakeholders to the organisation’s activities, identifying potential gaps between expectations and performance, developing risk scenarios from those gaps, and assessing their likelihood and possible adverse impacts on the organisation’s business model. However, it may be challenging to make accurate assumptions about stakeholder expectations, i.e. assumptions that are appropriately concrete and up to date, as stakeholders’ expectations may change over time and might not be homogenous even within a single group of stakeholders. Measuring performance gaps against assumed expectations therefore adds to the challenges.

4.2  Methods and Approaches

The following section offers general guidance for a reputational risk assessment workflow in a coherent and systematic manner, including anticipated changes to the control environment, in order to provide a forward-looking view and in order to manage and monitor reputational risk effectively over time. This is set within a “causal approach” to reputational risk assessment, which includes the components of risk identification (see section 4.2.2 of this paper), risk analysis (see section 4.2.3), and risk evaluation (see section 4.2.4).

4.2.1  Stakeholders’ Risk Assessment Methodology and Workflow

A starting point for a first-time exercise is to discuss and analyse reputational risks that have materialised in the past to understand their causes and consequences, what has been done to control the likelihood of the risks occurring, and to mitigate their consequences emanating from stakeholder reactions. Via this approach, shifting risk and potential future reputational risks can be explored.

The Bow-Tie Technique suggested here, in order to manage the risk assessment workflow, is well-suited to capture risk scenarios and to come to a meaningful analysis and aggregation of the reputational risk. Bearing in mind that the risk assessment exercise is a tool for risk management and decision-making, it is understood that the risk assessment results shall compare against risk limits and risk tolerance in order to determine which risks are acceptable and how risk limits and risk tolerance is understood in the context of the risk appetite (see section 3.1 for definitions of terms).

Illustration of the Bow-Tie Technique (Source: Berlin Risk, December 2018)

---

Copyright Berlin Risk 2019
A Decision-Making Tool: The Bow-Tie-Technique

Risk factors and indicators emanating from:
- Ownership structure
- Shareholder and management:
  - Commercial and political relationships
  - Business interests and behaviour
- Market dynamics:
  - Lack of trust:
    - Recent corporate failures
- Operational environment:
  - Corruption:
    - Reputation:
    - Financial:
  - Political:
  - Environmental:
    - Social and governance issues (ESG)
- Change in public opinion:
- Reputation:
- Association with sanctioned entities or individuals
- Inappropriate business associations
- Inappropriate business partners

Consequences:
- Stakeholder anger with negative consequences:
  - Loss of investors
  - Loss of project
  - Loss of control
  - Financial issues

Stakeholders may not be equally relevant for an organisation, and their expectations may not be uniform.

Causes and consequences:
- Likelihood and seriousness of a risk can vary, and they also depend on risk controls and mitigants in place.

Stakeholders and project:
- Reputational:
  -ハード:
  - Impact
- Internal:
  - Risks:
  - Control

International Organisations:
- Negative reporting
- Inclusion in blacklists
- NGOs and the media:
  - Negative campaigning

Counterparties:
- Termination
- Rejection of future collaboration
- Governments:
  - Legal obstacles
- Governments:
  - Access to international funding
- Financial institutions:
  - Limited access to international funding
- International:
  - Negative media reports
  - Negative lobbying

Co-investors:
- Loss of control
- Loss of project
- Loss of investment

Environmental:
- Social and governance issues (ESG)

Environmental:
- Social and governance issues (ESG)

Environmental:
- Social and governance issues (ESG)

Environmental:
- Social and governance issues (ESG)
4.2.2 Reputational Risk Identification

The following section sets out the first step of risk identification.

### Risk Sources

Sources of reputational risk are regarded as the main reputational risk criteria, relevant for a planned or on-going customer relationship:

- Customers located in a certain country or a number of countries, from which country specific risk can arise.
- Defined sectors bear specific risks. Additional sources of risk may include third parties and competitors that might attack an organisation, e.g. cyber criminals, and geopolitical players whose actions although not targeting the organisation specifically may have repercussions on the bank’s operations and projects and thus have an impact upon reputation.

### Lines of Business

All departments and lines of business that are competent to identify risks that arise from the sources mentioned above should implement the reputational risk assessment methodology. Any one department may face reputational risks from various sources, which may be relevant for assessing a particular reputational risk. The aim of this exercise is also to establish ownership for a certain reputational risk. One way to decide about ownership would be to determine who would be able to control or coordinate the control of the relevant risk causes in order to prevent the risk events from happening according to the Lines of Defence model. Risk ownership issues will be discussed later.

### Causes and Indicators of Risk

The causes of risk originate from the sources of risk and might lead to certain risk events. As mentioned above, in relation to the country source of risk, this could be a customer with links to government or a state-owned entity. As a consequence, certain stakeholders would generate negative publicity. It should be noted that the likelihood of a certain risk event occurring could depend on the coincidence of multiple causes, thus increasing complexity. Also, it is possible that the information about risk causes is uncertain, weak, or ambivalent, which makes assessing the reputational risk more difficult.

In order to support the assessment of ambiguous reputational risk, one should think of a cause of risk as arising from an issue of concern that could eventually evolve into a reputational risk, which would be relevant to a financial institution. Regarding customer risk sources, for example: Should a prospective partner be investigated for corruption or associated with criminal business practices, the findings would be of concern for reputational risk, which could evolve into a risk event that would associate the
organisation with potentially inappropriate behaviour. Certain stakeholders would enact consequences, which could have a significant impact on a project. Key risk indicators are useful for assessing issues of concern and monitoring reputational risk; however, such indicators are not necessarily suited to predict the likelihood and severity of risk events.

Internal Controls and Lines of Defence

Given that various causes of risk exist, the likelihood for each risk to materialise as an actual risk event also depends on the internal risk controls that an organisation has in place and which are applied preventively. A key role in internally controlling the causes of risks, and thus the likelihood of related risk events occurring, is set out according to the Lines of Defence model. Whenever guidance is required due to incomplete, ambivalent, and uncertain information regarding the causes of risk information, or because of disagreement about ownership of the risk (i.e. who is responsible for applying risk controls), the second Line of Defence should be involved. The same is true when causes of strategic risk are identified and require risk management decisions beyond regular risk control measures. Notably, the second Line of Defence would, however, also be responsible for alerting the 1 LoD of causes of risk, which are linked, for example, to the changing political, economic, or regulatory environment.34

Risk Events and Interconnected Risks

The scenarios of risks describing possible reputational risk events build the core of the reputational risk assessment methodology, as mentioned above. The identification of a reputational risk scenario should include all the possible events that could affect stakeholders and call them into action. This includes operational risk scenarios referring to possible internal gaps with respect to required legal, financial, and customer due diligence or transaction monitoring. An indicative list of relevant reputational risk events is provided below. As mentioned above, of particular concern are integrity risks events that pose a reputational risk for the organisation by association with inappropriate counterparties, so-called third-party risks.

Indicative list of Reputational Risk Events

<table>
<thead>
<tr>
<th>Risk Event Category</th>
<th>Risk Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational risk</td>
<td>– Failure of internal governance systems, rules and procedures, involving EU and international regulations and conventions, including data protection, data leaks</td>
</tr>
<tr>
<td></td>
<td>– Non-performing loans</td>
</tr>
<tr>
<td></td>
<td>– Involvement of customer in commercial dispute</td>
</tr>
<tr>
<td></td>
<td>– Implication of customer in regulatory scrutiny</td>
</tr>
<tr>
<td></td>
<td>– Internal fraud/embezzlement of funds, etc.</td>
</tr>
<tr>
<td>International legal risk</td>
<td>– Involvement with criminal counterparties (corruption, money-laundering, crimes against humanity)</td>
</tr>
<tr>
<td></td>
<td>– Involvement with sanctioned entities/individuals</td>
</tr>
<tr>
<td></td>
<td>– Association with terrorist financing</td>
</tr>
<tr>
<td>International regulatory risk</td>
<td>– Exposure to new EU/ international compliance regulations setting increased requirements for on-going and considered projects, etc.</td>
</tr>
</tbody>
</table>

34 Internal Audit usually builds the third Line of Defence.
Integrity risk
- Association with questionable politically exposed persons (PEPs)
- Association with questionable business partners and financial crime (including corruption, money laundering, fraud, and tax evasion)
- Association with opaque ownership structures, including in offshore jurisdictions, etc.

Political Risk
- Association with authoritarian regimes and negative human rights record
- Exposure to government populism, regulatory interventionism in relevant market/sector, detrimental macro-economic decisions
- Exposure to popular discontent, unrest, political violence, internal armed conflict, etc.

Social responsibility and sustainability risks
- Controversial impact on social cohesion, labour conditions, economic development, environmental protection
- Association with controversial policy objectives, technical innovations, etc.

Geopolitical and security risk
- Regional or international entanglements
- Involvement with international crisis and conflict, war
- Being affected by cyber attacks
- Exposure to organised crime

Competition risk events
- Exposure of project to new market developments
- Exposure of project to competing investment policies by other/co-financing institutions, etc.

Any one customer relationship can be affected by various reputational risk events, which are sometimes linked to each other. The identification of interconnected risk events should therefore be regarded as a key feature of any risk assessment, aiming at establishing a detailed risk mapping of a project. Interconnected reputational risks that mutually reinforce each other may be more difficult to control and therefore imply an increased likelihood. The Bow-Tie Technique is particularly suited to analyse multiple risks as well as interconnected risk events.

4.2.3 Reputational Risk Analysis

The following sections explain the risk analysis phase.

Stakeholders and Mitigants

Stakeholders are any group of people who might claim an interest in an organisation’s processes and whose actions could influence an organisation’s success. These include customers and counterparties, investors and financial institutions, employees, civil society organisations, the public, and the media. Should reputational risk events occur, stakeholders would be the actors who might impose relevant risk consequences depending on their motivation and resources. Taking into account which actions each affected stakeholder might take, the Bow-Tie Technique includes optional mitigation measures that aim to engage stakeholders, possibly reduce the intensity of their actions and the relevant consequences, and thus the risk impact emanating from reputational risk events. The example provided above demonstrates the importance of recognising affected shareholders, understanding their possible actions, preparing feasible mitigation measures, and anticipating ultimate risk consequences.
It should be noted that different stakeholders do not necessarily view reputational risk attached to a project in the same manner, and thus there might even be competing perceptions. For example, a bank might be willing to accept certain risks related to a customer in a country under authoritarian rule, but a civil society organisation might stage protests against such investments or campaign against adverse environmental outcomes. The stakeholder approach is particularly relevant for projects where specific reputational risk might be accepted under the condition of targeted risk mitigations measures. Such measures can include creating increased transparency regarding beneficial ownership structures, close monitoring of the customer, protection against third-party intervention, or risk communication aiming to secure stakeholder support.

Risk Consequences

Adverse risk consequences can be described as losses, but they may not be quantifiable losses. Although commercial organisations might be interested in calculating the impact of reputational risk on the valuation of a company, other organisations may be interested in whether a potential loss of credibility would have a major impact on the ability to fulfil their mandate. It is therefore, important to explore the consequences of risk events and what effect certain stakeholder actions might have on an organisation’s current and future operations. For example, a violation of US sanctions might lead to severe fines as well as limiting an organisation’s access to raise money in the US capital markets. In addition, other financial institutions, the media, and civil society organisations would denounce the bank’s involvement with sanctioned entities, leading to an overall loss of credibility and reputation.

Similar to potentially multiple causes of risk, a specific risk event may result in multiple consequences, including positive consequences that need to be carefully related to each other in order to assess their overall impact on an organisation’s mission. If an organisation has a mission to expand into certain markets, and doing so would benefit those markets, the strategic mission may also be exposed to reputational risk stemming from controversy about the integrity of third parties or political risk and thus lead to criticism, which would require risk mitigation.

Likelihood of Risk Event, Impact of Relevant Risk Consequences, and Risk Severity Matrix

The Bow-Tie risk assessment technique foresees that the likelihood of the risk event taking place should be determined once the extent of existing risk controls, which might reduce the probability of the risk event occurring, have been taken into consideration. Similarly, the impact of an actual risk event should be determined after taking into consideration to what extent existing mitigants might reduce the risk consequences. In other words, the ultimate likelihood and impact analysis focuses on assessing residual reputational risks.

Various options for measuring qualitative reputational risk, including a five-point scoring system, exist. A simple but feasible system is to assign a high, medium, or low probability to a risk event, and also to assign a high, medium, or low impact to risk consequences.

The resulting Risk Severity Matrix combines the likelihood and impact assessment and classifies the severity of a particular risk event, as set out below.
Reputational Risk Evaluation

The reputational risk assessment methodology will eventually serve as a decision-making support tool, in that the results of the risk analysis will help to establish appropriate levels of risk limits within each of the lines of operation. Developing such risk limits forms the main part of the risk assessments’ reputational risk evaluation. Some of the risk limits will have to be defined within the first Line of Defence. For reputational risk events that are owned by the various lines of business, setting the risk limits in the second Line of Defence may become a more challenging exercise, as they will need to weigh strategic and external risks, internal disagreements over risk analysis, and ambiguity regarding the likelihood and/or impact of particular risk events.

Moreover, a particular challenge in developing risk appetite limits might be posed by cognitive biases, which can distort rational risk decision-making even within groups. Methods to establish rational risk attitudes in complex and uncertain decision-making situations do exist and can be applied in order to support the risk appetite framework.
4.2.5 Internal Controls—Reputational Risk in the Context of the AML Audit Risk Model

As set out in the EBA’s guidelines, all parts of the internal audit function (IAF) should verify, in particular, the integrity of the processes ensuring the reliability of the institution’s methods and techniques, and the assumptions and sources of information used in its internal models (e.g. risk modeling and accounting measurements). It should also evaluate the quality and use of qualitative risk identification and assessment tools and the risk mitigation measures taken. The same guidelines note that the organisation’s internal control framework should be adapted according to the specificity of its business, its complexity, and the associated risks. In the case of reputational risk management, the IAF should ensure adequate identification, measurement, and mitigation of reputational risks related to the AFC function as well as compliance with laws, regulations, supervisory requirements, and the institution’s internal policies, processes, rules and decisions. All reputational risk management measures related to the AFC function should therefore be embedded in the overall risk management framework of the organisation and audited accordingly.

5 Outlook

Reputational risk has grown in importance in recent years, firstly due to the increasing number of global financial institutions that have been fined for weaknesses in their anti-financial crime programmes, and secondly as a result of organisations being criticised for failing to mitigate environmental, social, and governance risks appropriately. These weaknesses appear to be the result of narrowly defined processes that are not connected with one another and therefore not effectively mitigating the so-called indirect risks, which ultimately and cumulatively manifest themselves as reputational risks.

Given this context it is important to note that reputational risk management is not a stand-alone programme embedded in any one division but rather a function that needs to operate across the organisation and be embedded in a wider reputational risk assessment framework feeding into an Enterprise-wide Risk Management System. It is therefore important to ensure that the flow of information and linkage of processes from various divisions is facilitated adequately.

In her book, “The Silo Effect: The Peril of Expertise and the Promise of Breaking Down Barriers”, Gillian Tett discusses how working in silos can result in inadequate information and insufficient accountability or coordination. Given how anti-financial crime has evolved over the past 30 years, this has led to silos being established in numerous financial institutions, which need to be dismantled, and functions restructured in order to be able to effectively mitigate the reputational risks attached to financial crime in the first instance. This topic is very relevant for the topic of reputational risk management, as any endeavours in this regard can only be effective if implemented across an organisation in an open and transparent measure. New approaches combined with appropriately designed and implemented technology can add value and strengthen to the effectiveness of any reputational risk management programme.
6 Works Cited

The following sections outline key books and articles from trade publications, as well as official guidance published by regulators and industry associations. References to corporate websites and other online publications including social media are referenced in the respective footnotes only.

6.1 Books and Articles


6.2 Regulatory and Industry Guidance


Basel Committee on Banking Supervision. (July 2009). *Enhancements to the Basel II framework*.


