

# NON-FINANCIAL RISK CONVERGENCE AND INTEGRATION

BREAKING DOWN THE SILOS  
MARCH 2018

## AUTHORS

Ramy Farha, Partner

Allen Meyer, Partner

Evan Sekeris, Partner

Elena Belov, Partner

# EXECUTIVE SUMMARY

During the last ten years, non-financial risk management has grown significantly in importance, complexity, and resource allocation for financial institutions. The observation holds true for the multiple disciplines that fall under the broad non-financial risk umbrella, including operational, compliance, ethics and conduct, information technology (IT) and cyber, business continuity, fraud, money laundering, third party, and legal risks. These disciplines organizationally have often operated in silos. However, the silo approach has resulted in both ineffectiveness and inefficiency. Therefore, we believe there are opportunities to improve the management of these non-financial risks and associated costs by rethinking the approach to non-financial risk management across financial institutions.

Non-financial risk management has grown in prominence after a number of highly publicized process, system, and people failures leading to direct financial losses and reputational impacts suffered by financial institutions. While estimating total losses due to non-financial risks is difficult, reported operational risk losses from 2011 to 2016 totaled more than USD 250 billion<sup>1</sup>. Additionally, the regulatory scrutiny surrounding non-financial risk management has been significantly heightened by the recent regulatory actions related to topics such as money laundering, sales practices, and market manipulation.

Non-financial risk management has become more challenging due to the added complexity from rapid shifts in technology, extensive process automation, and greater dependence on systems instead of people. These changes in the way financial institutions do business have led to new risk exposures, whether in the form of denial of service attacks, data theft, or online fraud.

Given these multiple pressures, we see no surprise with the fact that the industry has rapidly responded by building out non-financial risk management capabilities. Most often, the build has been done by hiring more people, introducing additional controls, and developing new processes in an effort to cover all bases. In many cases, the result was larger non-financial risk functions with greater responsibilities, but not necessarily ones that are best organized to meet these challenges.

## In this paper we:

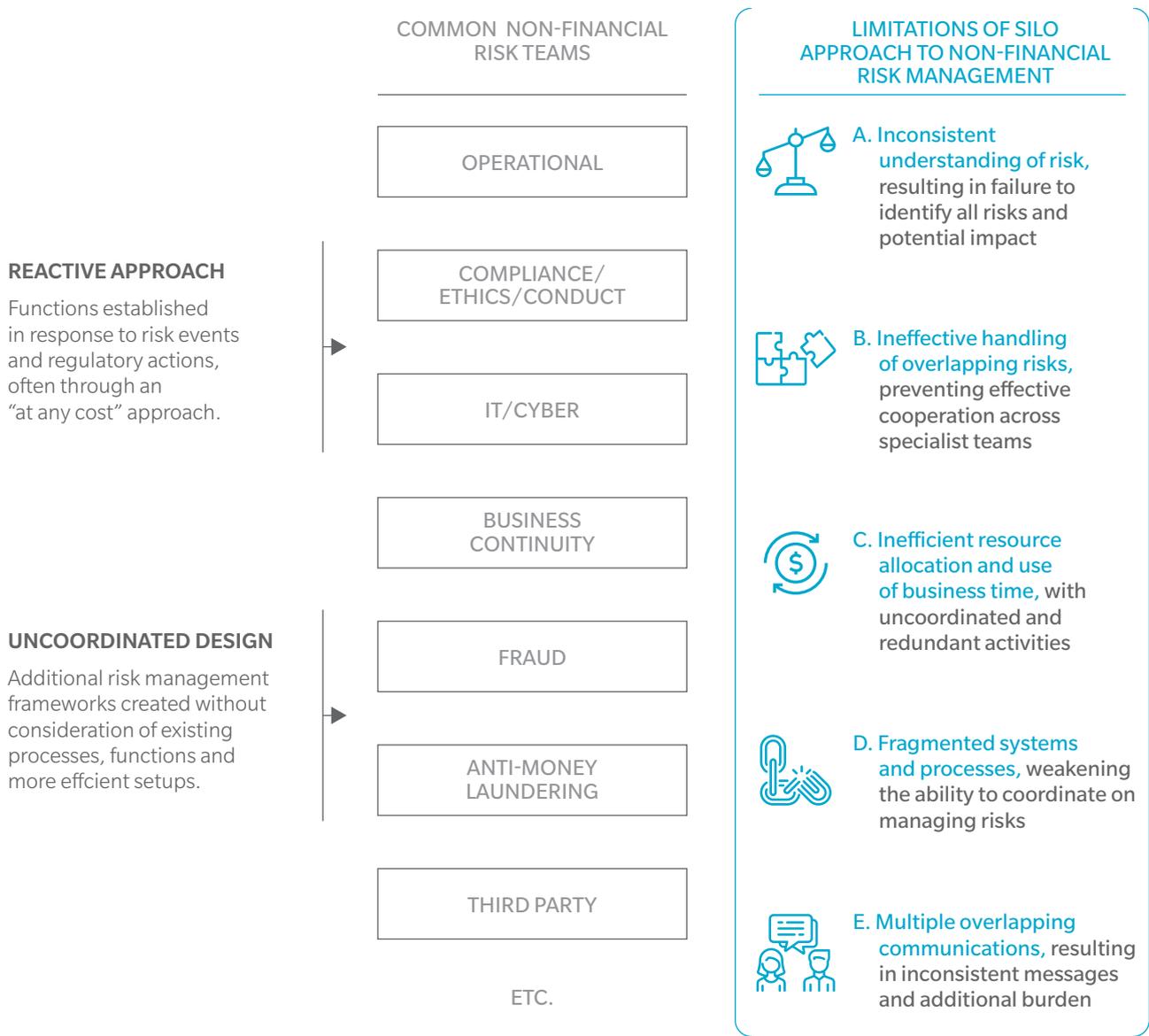
- **Discuss the limitations** of non-financial risk management approaches currently used by many financial institutions.
- **Propose strategies and actions** financial institutions need to consider and implement to create a more coherent non-financial risk management approach, and improve the effectiveness and efficiency across, primarily, oversight teams responsible for non-financial risk management.
- **Suggest adjustments to key processes and tools** used for non-financial risk identification, assessment, and reporting.
- **Address related talent management and teaming issues**, and offer solutions to broaden non-financial risk staff skillset and build effective non-financial risk management teams.

<sup>1</sup> ORX Banking report – November 2017

# NON-FINANCIAL RISK MANAGEMENT: LIMITATIONS OF CURRENT APPROACHES

Most organizations now have numerous specialist teams dedicated to the management of various non-financial risks, often with overlapping remits and different chains of command; an approach we will refer to as a ‘silo’ approach for the rest of the paper. The current approach of organizing the various teams exposes institutions to both ineffectiveness and inefficiency in non-financial risk management.

Exhibit 1: Current state of non-financial risk management



The limitations of the silo approach to non-financial risk management include:

#### **A. INCONSISTENT UNDERSTANDING OF RISK**

Individual teams are using risk taxonomies with inconsistent methodologies. For example: Compliance considers transaction reporting failure as the risk of breaching specific regulations, where as Operational Risk considers transaction reporting failure as a technology risk. The risk event can therefore be the same, but the event can be classified into different risk types and assessed differently depending on the oversight team. Overall, a poor understanding of risk can result in failing to identify all relevant risks, in conflating risks with impacts, or in having inconsistent business responses to the same risks.

#### **B. INEFFECTIVE HANDLING OF OVERLAPPING RISKS**

When multiple and overlapping types of risks are involved with an event, there is often a lack of clarity about which specialist team is responsible for what, which can significantly hinder the progress (for example, sales practices events involve operational, compliance, legal, ethics, human resources) and may lead to inconsistent risk responses by oversight teams.

#### **C. INEFFECTIVE RESOURCE ALLOCATION AND USE OF BUSINESS TIME**

Due to lack of visibility and coordination, specialist teams tend to issue redundant requests for information and materials to the business units, significantly decreasing the efficiency of operations (for example, different risk and control self-assessments conducted for Operational Risk and Compliance). Similarly, these efforts often lead to duplicative controls that add complexity and friction to business operations without offering a marginal reduction in risk.

#### **D. FRAGMENTED SYSTEMS AND PROCESSES**

Specialist teams often use separate systems, processes, and tools to assess, measure, monitor, and report on risk. These fragmented systems and processes limit the ability to coordinate the management of overlapping risks across these teams, leading to the inefficient use of time and sub-optimal solutions. The outcome can be a failure to identify and report on risks, and/or to set up proper controls to manage these risks.

#### **E. MULTIPLE OVERLAPPING COMMUNICATIONS**

Specialist teams often provide multiple and sometimes overlapping communications that may contain inconsistent messages and increase the challenge of obtaining a good understanding of the overall risk picture. As these communications can contain similar content, the burden on senior management and the Board to process and react to the information increases, potentially providing inconclusive or conflicting recommendations to act upon. For example, senior management may receive reports from Anti-Money Laundering, Cyber Risk, and Operational Risk that identify the top risks within each individual discipline, but do not necessarily enable easy comparison or understanding of how the risks compare using a common scale.

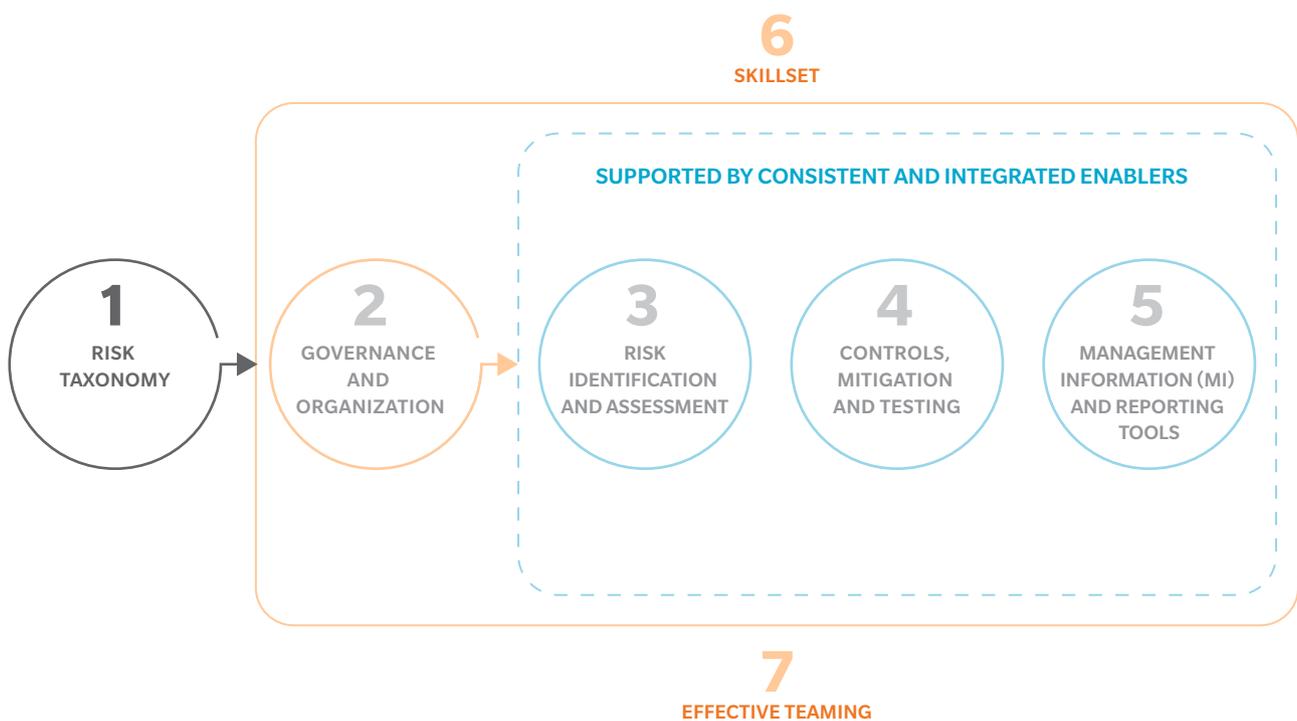
# NON-FINANCIAL RISK MANAGEMENT: PROPOSED NEW APPROACH

The shortcomings of a “silo” approach significantly constrain the effectiveness and efficiency of non-financial risk management. Financial institutions must start looking for ways to improve the approaches taken by specialist teams to non-financial risk management.

Our recommendation is to divide the path to integration and convergence of non-financial risk management into seven components (see Exhibit 2). An effective starting point is the development of a mutually exclusive and comprehensively exhaustive risk taxonomy to drive both governance and organization, and to serve as the foundation for the rest of the non-financial risk management components. Specifically, the risk taxonomy drives risk identification and assessment; controls, mitigation, and testing; and management information (MI) and reporting tools. On top of these components, a critical factor is for staff to have broad and adaptable skillset and for effective teaming to exist among specialist teams.

The remainder of the section discusses these seven components and outlines the foundations of an approach to significantly reduce some of the pain points experienced by financial institutions today related to non-financial risk management.

Exhibit 2: Non-financial risk convergence and integration components

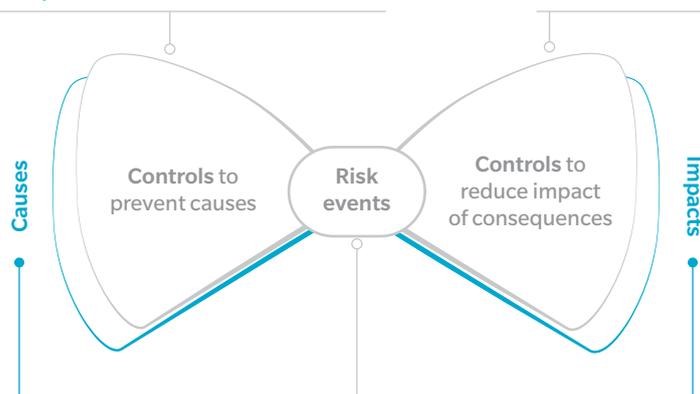


# 1. BUILD A SINGLE NON-FINANCIAL RISK TAXONOMY

Financial institutions should aim to set up a single, rationalized taxonomy that ensures consistency, comprehensive coverage, and sufficient clarity and granularity to resolve the problems resulting from using inconsistent and insufficiently granular taxonomies. The risks in the taxonomy should be actual risk events, not causes of or impacts from these events. Exhibit 3 illustrates these differences and the importance of ensuring the taxonomy captures the discrete event that occurred, rather than what gave rise to the event or the ultimate consequences the event had.

Exhibit 3: Bow tie non-financial risk methodology

- Preventive or detective controls may be used to prevent root causes from leading to a risk event
- Cause identification may help define appropriate controls
- **E.g. Leverage cloud services to improve bandwidth and deter attacks**
- Specific controls may be used to mitigate the impact of a realized risk event
- **E.g. Crisis Management response following event with Reputational Risk**



- |   |   |  |
|---|---|--|
| <ul style="list-style-type: none"> <li>• A cause gives rise to an event</li> <li>• Defined in terms of the underlying causes, i.e., the environment that allows risks to develop</li> <li>• Multiple causes can be mapped to an event</li> <li>• <b>E.g. Bank IT systems are antiquated encouraging external fraud</b></li> </ul> | <ul style="list-style-type: none"> <li>• Discrete, specific occurrence that has an impact on the institution</li> <li>• Used as unique identifier</li> <li>• Risk event needs to have an immediate impact</li> <li>• <b>E.g. Bank website is taken down by a distributed denial of service attack (DDoS)</b></li> </ul> | <ul style="list-style-type: none"> <li>• Specific outcome of the event</li> <li>• Can be financial, regulatory, legal, or reputational, must be measured in a consistent way to allow comparison</li> <li>• Multiple impacts can be mapped to a single event</li> <li>• <b>E.g. Bank reputation as being secure is tarnished following the attack</b></li> </ul> |
|---|---|--|

There are a number of guiding principles that financial institutions should be aware of when defining a common taxonomy, which include:

- Risk types are mutually exclusive and collectively exhaustive.
- Risk definitions are comprehensive in scope.
- Risk taxonomy is simple and intuitive for end-users.
- Risk taxonomy considers the specific risks that the institution may be subject to – both today and in the future.
- Risk categories can be tied back to specific laws, rules, and regulations.

Exhibit 4: Example granular break-down of non-financial risks

INCREASING LEVEL OF GRANULARITY			
LEVEL 1	LEVEL 2	LEVEL 3	LEAD STAKEHOLDER
1 Internal fraud	1.A Internal system security willful damage, theft or fraud	1.A.i Internal theft or fraud through system intrusion and/or unauthorized access to technology infrastructure	A lead team should be assigned to each risk type
		1.A.ii Internal virus, malware, denial of service attack	
		1.B.i Bribery and corruption	
	1.B Internal theft or fraud without system intrusion	1.B.ii Unjust enrichment, misappropriation or theft of firm assets and information	
		1.B.iii Unjust enrichment, misappropriation or theft of client assets and information	
		1.C.i Insider trading	
	1.C Unauthorized activity	1.C.ii Rogue trading	
		1.C.iii Market manipulation	
		2.A Employee relations	
2 Employment practices and workplace safety	2.B Employment diversity and discrimination	2.B.i Harassment and intimidation	
		2.B.ii Non-diverse and discriminatory employment policies and practices	
	2.C Safe workplace environment	2.C.i Employee injuries and workplace design violations	
		2.C.ii Public health and safety breaches	
3 Execution, delivery and process management	3.A Reporting error or failure (non-regulatory)	3.A.i Internal misreporting	
		3.A.ii ...	
	3.B Third party risk	3.B.i Financial failure of third party	
		3.B.ii ...	

Individual risks are linked to specific laws, rules, and regulations as appropriate

BENEFITS OF A NON-FINANCIAL RISK TAXONOMY

Developing a common risk taxonomy with a greater level of granularity requires significant effort and coordination among the multiple impacted areas. For example, there may be a challenge to draw the line between the scope of specific risks, such as certain types of fraud and anti-money laundering (AML). However, achieving a single risk taxonomy delivers several benefits such as:

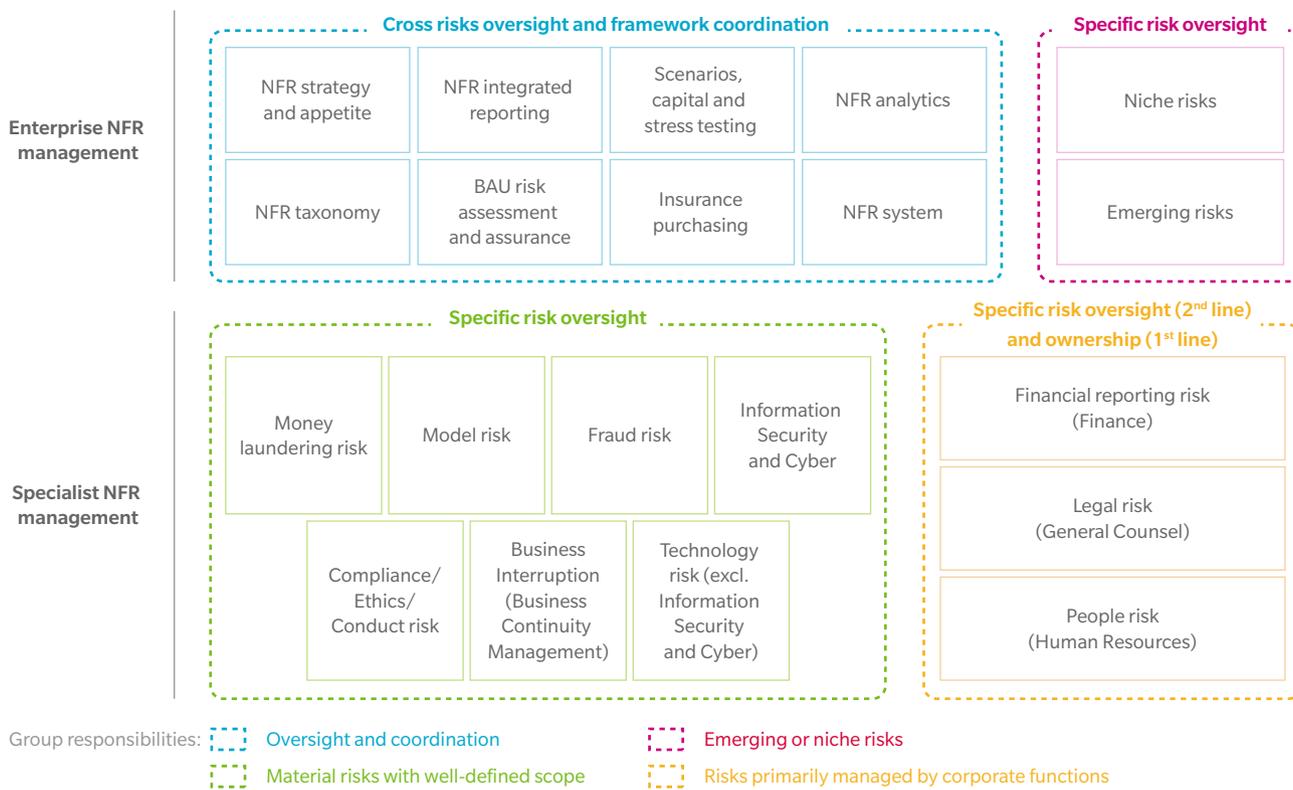
- Facilitates the development of an organizational structure driven by a common understanding of non-financial risk types.
- Reduces the risk exposure by enabling identification, monitoring, and management of common non-financial risks across functions as nomenclature and definitions are aligned.
- Increases efficiency and effectiveness by reducing the duplication of management of non-financial risk types, enhancing communication across teams, and enabling the rationalization of key controls

## 2. DRIVE A STRATEGIC NON-FINANCIAL RISK GOVERNANCE AND ORGANIZATIONAL FRAMEWORK

Financial institutions should leverage the risk taxonomy to clearly articulate the governance and organization of different non-financial risk functions to minimize overlaps and gaps. While there is no one-size-fits-all model, we believe the target governance and organization should be based on the following broad layers (see Exhibit 5):

- **Enterprise non-financial risk (NFR) management teams**, responsible for oversight and coordination of all non-financial risks, effectively own the NFR management framework and centralize select shared services (such as NFR data analytics and NFR reporting). In addition to these cross-risks roles, the group is responsible for independent oversight of specific material risks that span multiple functions and emerging and/or niche risks.
- **Specialist NFR management teams**, responsible for oversight and challenge for the most significant and well-defined risk types, such as money laundering, fraud, compliance, ethics, and conduct risks. Specialists are responsible for risk-specific activities, such as defining and testing controls; and providing risk assessment, training, change management, and advice. Some areas may have dual roles as first and second lines of defense as the risks managed are closely linked with core activities (such as people risks managed by the Human Resources function), and as such, responsibilities must be clearly delineated.

Exhibit 5: Illustrative future non-financial risk organizational model



## BENEFITS OF STRATEGIC NON-FINANCIAL RISK GOVERNANCE AND ORGANIZATION

Developing an organizational and governance model delivers both cross-functional coordination of activities and appropriate focus on individual risk types. As is the case for any significant organizational change, designing and implementing such a model has implicit challenges. However, implementing a strategic governance and organization delivers several benefits such as:

- Helps financial institutions develop better governance around non-financial risks.
- Allows to limit duplication of work between non-financial risk functions.
- Minimizes the risk of having gaps in terms of the risk types covered by the non-financial risk framework.

### 3. STREAMLINE NON-FINANCIAL RISK IDENTIFICATION AND ASSESSMENT METHODOLOGIES

Financial institutions should aim to set up a common methodology for non-financial risk identification and assessment, and coordinate these processes and the regular communication within units to reduce workload and burden on the business. A common methodology is supported by a standardization of the scales used to determine the likelihood and impact of risks. For example, as illustrated in Exhibit 6, common likelihood and impact scales can be developed and used across all non-financial risk types.

## Exhibit 6: Example non-financial risk common likelihood and impact scale

### ILLUSTRATIVE GUIDELINES FOR ASSIGNING IMPACT OF RISK

	Very low	Low	Moderate	High	Critical
<b>Financial impact</b>	Less than \$WW million	Approximately \$WW to \$XX million	Approximately \$XX to \$YY million	Approximately \$YY to \$ZZ million	Losses greater than \$ZZ million
<b>Reputational impact</b>	No reputational exposure or harm	Localized negative media coverage that does not materially impact brand value	Negative media coverage across multiple jurisdictions and/or loss of client confidence	Negative media coverage on a global basis and/or widespread loss of client confidence	Sustained negative media coverage on global basis and/or loss of key client(s)
<b>Regulator interest</b>	No known regulator interest	Regulator has shown some interest in publications and conferences	Regulator is highly focused on the risk	Regulator is highly focused on the risk, specific to the applicable industry	Regulator is highly focused on the risk and has made an inquiry to the bank

**Factors for consideration:**

- **Financial :** Fines/penalties, loss of revenue (disgorgement), client prohibition, cost of remediation, credit/liquidity issues, potential for systemic impact
- **Reputational:** Duration and scope of negative media coverage, decrease in brand value, ability to prospect talent, ability to prospect target clients, potential for systemic impact

### ILLUSTRATIVE GUIDELINES FOR ASSIGNING LIKELIHOOD OF RISK

	Very unlikely	Unlikely	Somewhat likely	Likely	Very likely
<b>Frequency</b>	One occurrence every 5 years or less	More than one occurrence every 5 years but less than one occurrence per year	One to three occurrences per year	Occurs quarterly or more often but less than weekly	Occurs weekly or more often
<b>Complexity</b>	Not complex				Very complex
<b>Nature</b>	Automated				Very manual
<b>Volume</b>	Low				Very high

## BENEFITS OF STREAMLINING NON-FINANCIAL RISK IDENTIFICATION AND ASSESSMENT

Adopting a common self assessment framework across non-financial risks, which is further reviewed and enriched by individual specialist risk teams for additional oversight perspectives, will benefit financial institutions. For example, Third Party risk team conducting vendor risk assessment and Cyber Risk team conducting penetration tests/attack simulations. However, regardless of the specific approach, streamlining non-financial risk identification and assessment delivers several benefits such as:

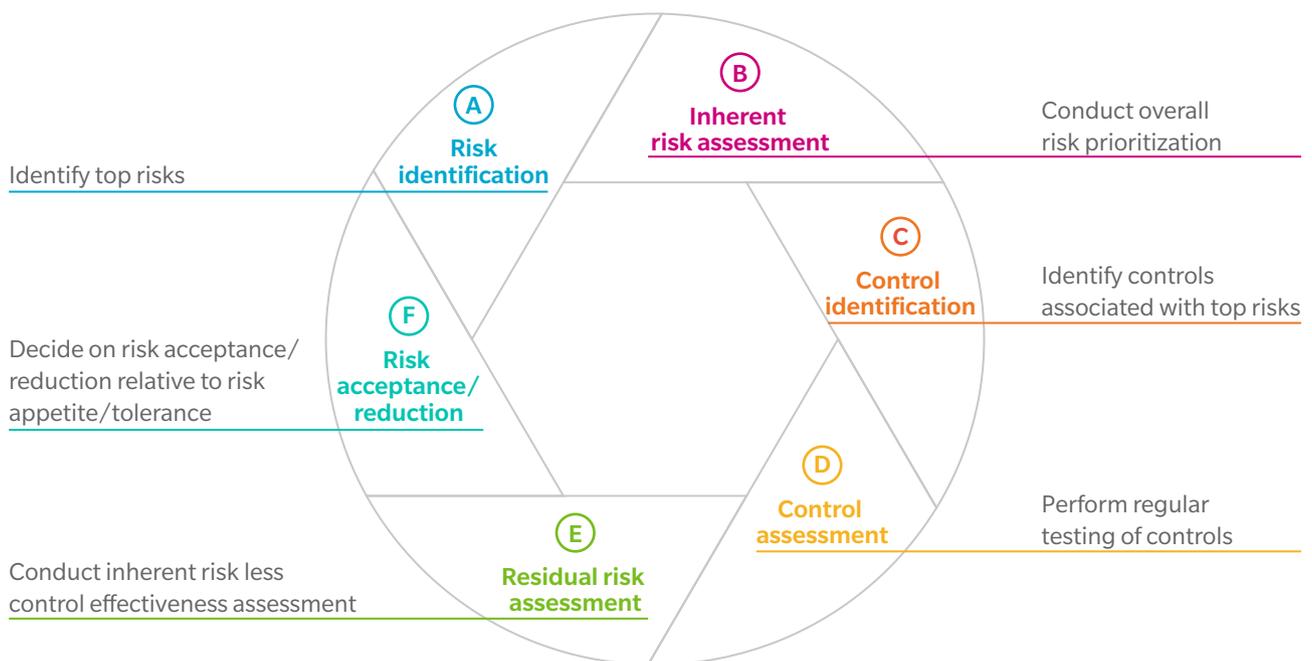
- Removes duplication in activities, especially when interacting with front line units.
- Provides a comparable view of likelihood and materiality across different non-financial risk types.
- Ensures a consistent understanding of non-financial risk throughout the organization, especially since many of the risk identification and assessment activities support a number of downstream processes, including reporting.

## 4. INTEGRATE NON-FINANCIAL RISK CONTROLS, MITIGATION, AND TESTING

Financial institutions should better integrate risk and controls management to ensure a link between the overall risk materiality and the dedicated control efforts. As illustrated in Exhibit 7, controls need to be closely aligned to the risk identification and assessment processes to ensure the key risks are covered and that the controls are appropriate.

Exhibit 7: Integrated non-financial risks and controls

THE INTERNAL CONTROL FRAMEWORK HAS SIX IDENTIFIABLE STEPS



### BENEFITS OF INTEGRATED NON-FINANCIAL RISKS AND CONTROLS

Integrating risks and controls delivers several benefits such as:

- Helps firms to more appropriately designate key controls and set up appropriate testing procedures.
- Allows firms, once the integration is complete, to rationalize the total number of controls in place in order to manage the various risks, remove duplicative controls, and ensure proportionality of the control relative to the risk.
- Helps ensure the controls are as effective as possible and set up in the most efficient way to lower the risk to the organization.
- Facilitates the creation of a centralized group focused on integrating the testing framework and ensuring there are common methodology, reporting templates, escalation, and rating systems in place.

## 5. DESIGN A SINGLE NON-FINANCIAL RISK DATA REPOSITORY AND REPORTING SYSTEM

Financial institutions should aim to create a common data repository and reporting system, as well as a centralized issue tracking system to support non-financial risk management processes – including risk assessments, controls, metrics, and testing outcomes. Therefore, financial institutions should integrate a suite of technology-enabled non-financial risk management tools to provide the capabilities necessary for collaboration across non-financial risk functions.

However, implementing a comprehensive IT system and associated tools will not be a silver bullet that automatically solves other underlying problems in the framework. As illustrated in Exhibit 8, system and tools can help augment a strong existing framework and make the framework more effective, but cannot fix underlying problems, for instance, related to taxonomy or processes. Similarly, a crucial step is to ensure the right people are hired, trained and given the opportunity to work efficiently across teams, even with a market-leading IT system and associated tools in place.

---

### Exhibit 8: Implementing a non-financial risk IT solution is not a silver bullet

#### NON-FINANCIAL RISK IT SYSTEM AND TOOLS CAN:

- ✓ Facilitate sharing of information
- ✓ Increase efficiency
- ✓ Automate mechanical processes
- ✓ Provide tools for risk analysis
- ✓ Help track issues/mitigation actions
- ✓ Centrally store data

#### BUT CANNOT:

- ✗ Provide best practice risk/controls language
- ✗ Provide best practice risk/controls processes
- ✗ Identify issues or control weaknesses
- ✗ Mitigate issues or implement controls
- ✗ Replace human judgment

---

### BENEFITS OF SINGLE NON-FINANCIAL RISK DATA REPOSITORY AND REPORTING SYSTEM

Implementing a unified non-financial risk IT system and associated tools delivers several benefits such as:

- Achieves significant efficiency savings once data collection is coordinated given data and results are gathered only once and limit work duplication.
- Ensures there is a consistent “one source of the truth” of non-financial risk data.
- Allows reporting to be consistent in terms of content and to be created based on automated processes, which helps to improve the messaging and communication to management and the Board, and avoids the dissemination of conflicting messages.
- Facilitates collaboration across non-financial risk functions for processes such as issue reporting, data collection, and root cause analysis and lessons learned.

## 6. PLAN FOR FUTURE NON-FINANCIAL RISK WORKFORCE TRANSITION

Financial institutions should focus on understanding what capabilities will be required for future Risk organizations (see Exhibit 9) and put in place a plan to enable the workforce transition – for example, adapt career planning, talent acquisition, and training. Currently, Risk functions often suffer from having non-financial risk talent with a specific, narrow set of skills. Future non-financial risk managers need to have a broad range of non-financial risk expertise, including a focus on strategic and principles-based management, a more predictive rather than forensic mindset, and significant abilities to work in teams and collaborate across non-financial risk types.

Exhibit 9: Shifting expectations: Risk professional of the past to risk professional of the future

Past	Future	Business context
Tactical and transactional	→ Strategic	Changing risk profiles require professionals with multiple skills (for example, interaction of different risks, importance of data and analytics)
Depth of knowledge	→ Depth and breadth of knowledge	
Forensically minded	→ Predictively minded	
Largely siloed interaction	→ Breaking of silos	Maximizing efficiency and ensuring coordination of NFR risk management across the different specialist areas
Individualistic	→ Collaborative	Governments, regulators and customers want good banks that do the right thing, focusing on broad conduct and increased consumer protection
Rule focused	→ Principles focused	
Autocratic	→ Accountable	

Source: Oliver Wyman

### BENEFITS OF NON-FINANCIAL RISK TALENT MANAGEMENT STRATEGY

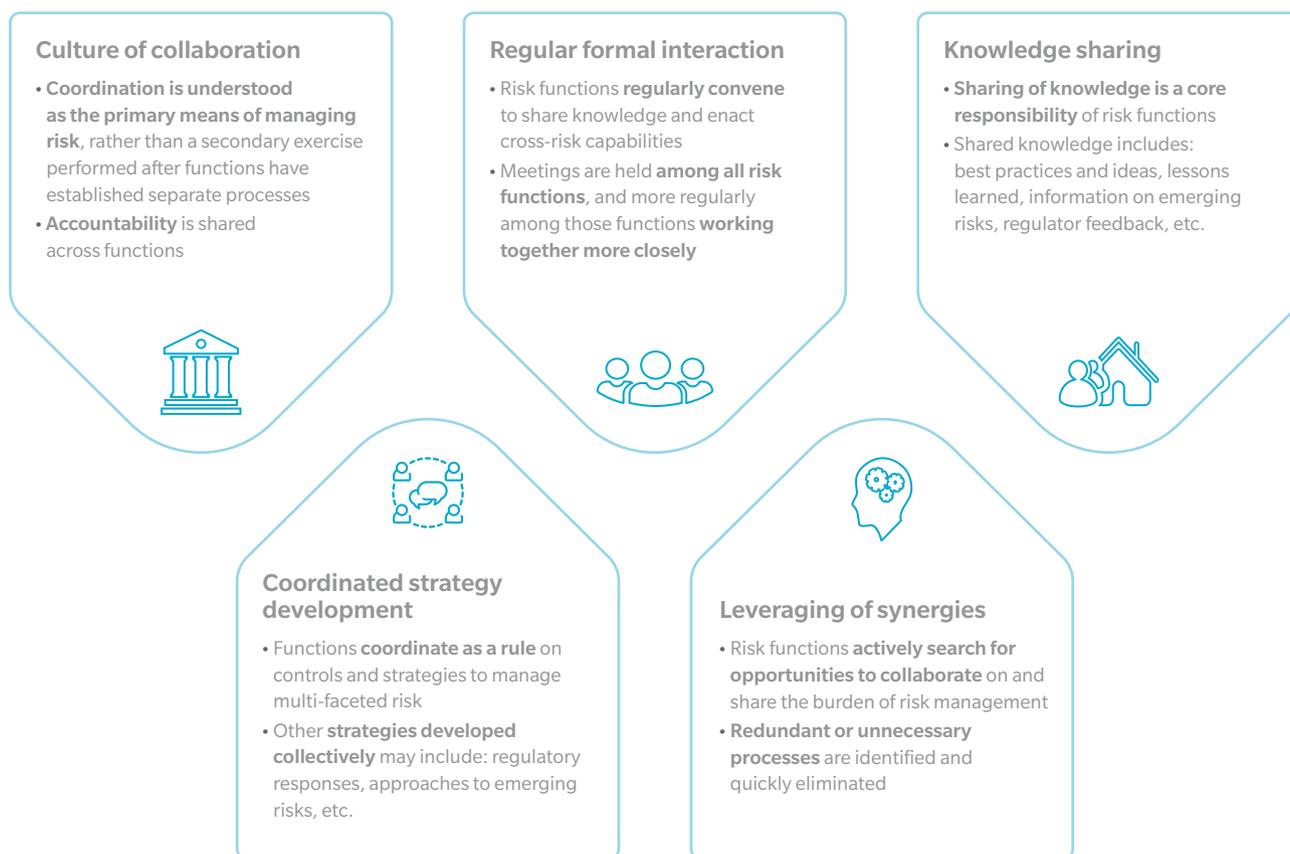
Putting such talent management strategy in place achieves several benefits such as:

- Makes non-financial risk roles more attractive to candidates.
- Helps to improve the value these candidates provide to the overall organization.
- Enables the non-financial risk function to better leverage shifts in technology, greater data proliferation and sophisticated analytical capabilities, which are driving significant transformation in how non-financial risk management is done.
- Helps the organization better manage the new types of non-financial risks that emerge from the changes stemming from the transformation of the way the overall financial services sector operates and the products and services provided.

## 7. BUILD EFFECTIVE NON-FINANCIAL RISK TEAMS

Financial institutions should be motivated to invest in the organizational elements that will help ensure that specialist teams are coordinating, collaborating, and sharing information. As illustrated in Exhibit 10, we see five key enablers of effective teaming. Core to these enablers is ensuring regular interaction and coordinated strategies of the teams to develop a formal framework in which to cooperate. In addition, organizations should foster a culture where collaboration, knowledge sharing, and leveraging best practices and synergies is actively encouraged and continuously enforced.

Exhibit 10: Key enablers of effective teaming



### BENEFITS OF EFFECTIVE NON-FINANCIAL RISK TEAMING

Developing a framework for non-financial risk teaming achieves several benefits such as:

- Enables organizations to overcome many of the drawbacks of a “silo” approach, including limiting redundant work efforts and ensuring clear roles for accountabilities.
- Supports innovation, where firms are able to efficiently solve non-financial risk management issues by bringing together the best ideas from across the organization.

# THE PATH FORWARD: NEXT STEPS FOR FINANCIAL INSTITUTIONS

As financial institutions look to move towards a more converged and integrated management of non-financial risks, we propose the following set of actions to help on the journey.

TOPICS	PROPOSED ACTIONS
<b>1. Build a single non-financial risk taxonomy</b>	<ul style="list-style-type: none"> <li>Review existing taxonomies used across Risk, Compliance, and related non-financial risk teams.</li> <li>Agree on a singular taxonomy with mutually exclusive and comprehensively exhaustive components and clearly defined levels of granularity.</li> </ul>
<b>2. Drive a strategic non-financial risk governance and organizational framework</b>	<ul style="list-style-type: none"> <li>Analyze current roles and responsibilities across non-financial risk groups to understand any duplication/overlap.</li> <li>Consider re-organization over time based on Enterprise NFR teams and Specialist NFR teams.</li> </ul>
<b>3. Streamline non-financial risk identification and assessment methodologies</b>	<ul style="list-style-type: none"> <li>Develop a consistent approach and coordinated timelines for risk identification and assessment across non-financial risks.</li> <li>Harmonize the level of granularity and use consistent rating scales for likelihood and impact across non-financial risks.</li> </ul>
<b>4. Integrate non-financial risk controls, mitigation, and testing</b>	<ul style="list-style-type: none"> <li>Perform a detailed review of the non-financial risk controls inventory to understand potential redundancies and duplicative controls.</li> <li>Develop a process aligning the controls to the risks identified to improve alignment of risks and controls.</li> </ul>
<b>5. Design a single non-financial risk data repository and reporting system</b>	<ul style="list-style-type: none"> <li>Review current non-financial risk technology solution to comprehensively cover the various non-financial risk types and the different tools/ activities involved with non-financial risk management</li> <li>Develop integrated solutions for any new non-financial risk systems developments to minimize manual tasks and repeat work</li> </ul>
<b>6. Plan for future non-financial risk workforce transition</b>	<ul style="list-style-type: none"> <li>Work with HR to develop medium-term target state capabilities for the non-financial risk teams.</li> <li>Develop training plans and adjust qualifications for hiring purposes to shift non-financial risk skillset towards target.</li> </ul>
<b>7. Build effective non-financial risk teams</b>	<ul style="list-style-type: none"> <li>Assess current ability to effectively team up across non-financial risk functions.</li> <li>Agree action plan to begin implementing elements of an effective non-financial risk teaming framework (for example, knowledge-sharing sessions, joint strategy development, adjustment to joint accountabilities for goals).</li> </ul>

While we do see some financial institutions dedicating efforts to improve convergence and integration of non-financial risk management, there is still significant work to be done to fully reap the benefits, and to truly provide comprehensive and value-adding risk management to the organization.

Financial institutions need to create a cohesive and comprehensive approach to the management of all non-financial risks. Such approach helps to improve the risk profile understanding, delivers significant efficiency gains for both the first and the second lines of defense, augments the governance and auditability of the underlying non-financial risk processes, achieves greater business engagement, and better crystallizes the value of non-financial risk management.

## ABOUT THE AUTHORS

Ramy Farha, Partner in the Finance & Risk and Public Policy Practices  
ramy.farha@oliverwyman.com

Allen Meyer, Partner in the Finance & Risk and Public Policy Practices  
allen.meyer@oliverwyman.com

Evan Sekeris, Partner in the Finance & Risk and Public Policy Practices  
evan.sekeris@oliverwyman.com

Elena Belov, Partner in the Finance & Risk and Organizational Effectiveness Practices  
elena.belov@oliverwyman.com

The authors would like to acknowledge and thank Kaja Pergar, Daniel Hermansson,  
and Rodrigo Gouvea for their valuable contributions.

[www.oliverwyman.com](http://www.oliverwyman.com)

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at [info-FS@oliverwyman.com](mailto:info-FS@oliverwyman.com) or by phone at one of the following locations:

### AMERICAS

+1 212 541 8100

Copyright © 2018 Oliver Wyman

### EMEA

rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and  
+44 20 7333 8333

### ASIA PACIFIC

+65 6510 9700