OLIVER WYMAN

Financial Services

RISK IDENTIFICATION
WHAT HAVE BANKS BEEN MISSING?

AUTHORS

Dov Haselkorn, Partner

Ilya Khaykin, Partner

Ross Eaton, Principal

MARSH & McLENNAN COMPANIES

INTRODUCTION

Risk identification is the process of taking stock of an organization's risks and vulnerabilities and raising awareness of these risks in the organization. It is the starting point for understanding and managing risks – activities central to effective management of financial institutions. However, many legacy risk identification processes have not fully served institutions' risk management needs, particularly those related to firm-specific stress testing and identification of the firm's largest vulnerabilities. These processes were not sufficiently comprehensive and deep enough – failing to highlight key underlying drivers of risks. This, in turn, led to critical gaps in risk management. US regulators have taken note and have been pushing institutions to expand and enhance their risk identification processes, and clearly link risk identification to stress testing and broader risk management activities.

Risk identification processes have not fully served institutions' risk management needs, particularly those related to firm-specific stress testing

Risk identification processes have traditionally centered on the key risk types of credit, market, operational and liquidity risk. Within each, risk subtypes are defined and categorized, often through a process that stays within the risk management organization. This approach to risk identification is aligned with the traditional, primary mechanisms for measuring risk and capital adequacy; both Risk-Weighted Asset (RWA) and economic capital approaches categorize risks similarly and implement specific analytical approaches to each risk type.

However, a new risk and capital management paradigm has emerged. This paradigm is based on enterprise-wide stress testing rather than relying primarily on traditional RWA and economic capital measures, which often use opaque models that can be difficult to link to observed real world conditions. The new paradigm instead involves defining a plausible but severe forward-looking scenario, then conducting a comprehensive assessment of how an institution would fare in this environment. Supervisors design mandatory stress scenarios that test common firm-level risks as well as key systemic vulnerabilities. However, each firm is also expected to develop a comprehensive stress scenario that is explicitly designed to target its own vulnerabilities. Pushed to develop meaningful scenarios, CCAR institutions have started to assess their vulnerabilities much more seriously. These new requirements have now arrived for Foreign Banking Organizations (FBOs) in the US and certain non-bank Systemically Important Financial Institutions (SIFIs) that will become subject to similar stress testing requirements soon.

Risk identification approaches are being pushed to adapt to these new requirements as well as address historical weaknesses observed at financial institutions. Institutions often did not effectively identify and assess a number of the risks that emerged before, during and since the crisis, for example:

- Strategic defaults on mortgages
- Mortgage repurchase risk
- Loss of market liquidity for many traded credit products
- Liquidity risk from rapid loss of secured funding and collateral calls
- Litigation arising from alleged fraud and misrepresentation of structured products

- Ratings downgrade-related risks
- Wide-scale outrage and reputational effects from the crisis

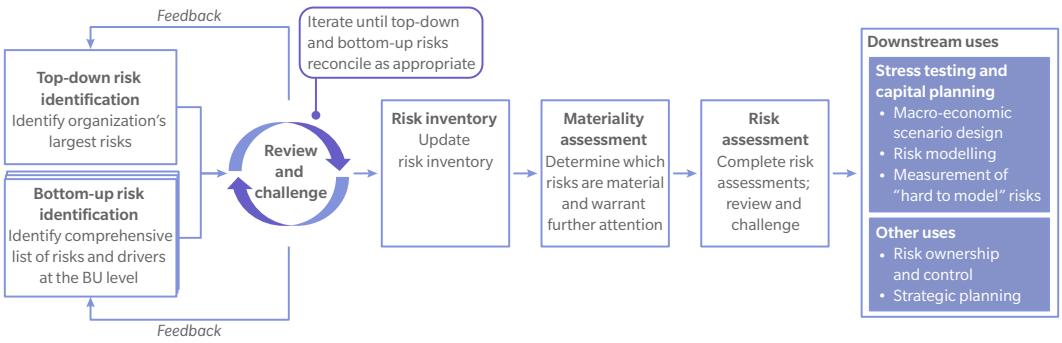
Traditional risk identification processes do not incorporate enough different perspectives on risks from across the organization; effectively distinguish the most significant risks from more minor risks; or sufficiently consider the underlying drivers of risks and how they could interact and amplify risks, or how minor risks might become severe in certain environments. As institutions adopt stress testing-based approaches to risk and capital management and work to develop stress scenarios specific to their own vulnerabilities, risk identification approaches must evolve to enable institutions to better understand their vulnerabilities, and to mitigate or capitalize against them.

THE NEED FOR RISK IDENTIFICATION

Risk identification is foundational to risk management in financial institutions. Transparency into the nature of risks drives downstream applications including risk measurement, control, and mitigation, as well as business planning, performance measurement and pricing. Key downstream uses of risk identification include:

- **Stress test scenario design**: risk identification should inform stress test scenarios to ensure the organization's key vulnerabilities are tested. For example, where a bank has a significant concentration of credit exposure to a specific industry, it may need to include an additional stress on factors which drive that industry's credit losses (e.g. sharp decline in metals prices increases default risk for mining companies) to better assess the extent of the risk.
- **Risk modeling and measurement of "hard to model" risks**: granular identification of risks helps verify whether models are able to effectively capture risks. In cases where complexity or data limit the ability to model a risk (e.g. reputational or strategic risks), risk identification can aid measurement through identification of a narrative of how the risks might materialize in a plausible event with severe consequences.
- **Risk ownership and control**: significant risks should be assigned owners – if they do not exist already – responsible for measuring, reporting and controlling these risks.
- **Strategic planning**: risk identification can inform the strategic planning process by highlighting key risks to the plan and how alternative strategic actions might affect the downside risk

Exhibit 1: Risk identification processes and downstream uses

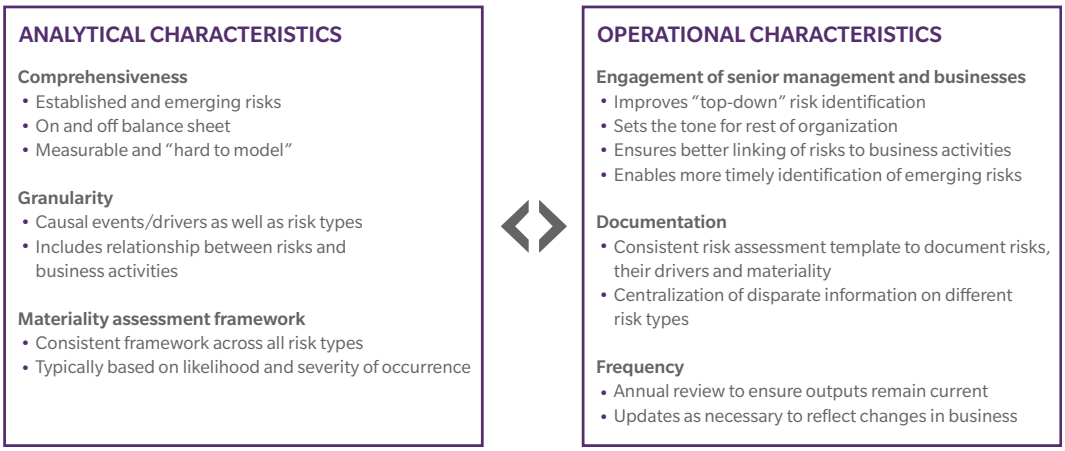


Source: Oliver Wyman Analysis

KEY REQUIREMENTS OF RISK IDENTIFICATION TODAY

These more advanced applications of risk identification have significantly upped the demands on risk identification processes. There are two categories of requirements: analytical characteristics and operational characteristics.

Exhibit 2: Key requirements for a robust risk identification process



Source: Oliver Wyman Analysis

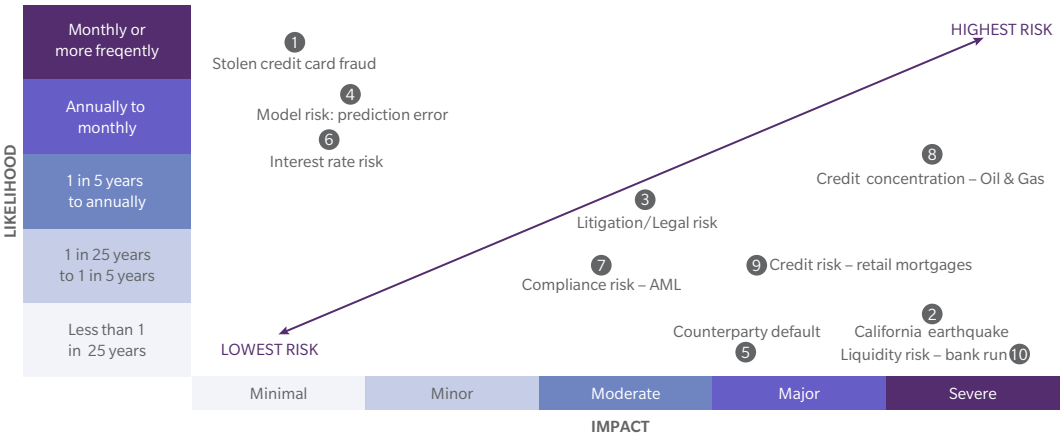
First and foremost, an institution's risk identification process must be comprehensive in its coverage of risks, including across small but quickly-emerging risks as well as risks with weaker risk measurement. Risk identification must also extend beyond the traditional categories of credit, market, operational and liquidity risks. Stress testing demands an understanding of not only loss drivers but also revenue and expense drivers, such as loan origination volumes, trading volumes, new debt/equity issuance by the bank's clients, etc. Broad capture of risks helps to ensure the institution has sufficient capital and liquidity, can appropriately tailor scenarios to its own risk profile, and can manage its risk appropriately. These broad, detailed risks should then be aggregated along a pre-defined hierarchy in order to bring them to a level which can be broadly understood and meaningfully discussed.

The output of new risk identification processes must also be much more thoughtful, and is qualitatively different from what is typically in place today. In addition to describing categories of risks, it must describe their specific fundamental drivers and the underlying conditions that give rise to losses resulting from these risks. For example, a specific systemic event such as the circa-2011 Euro area sovereign debt crisis saw not just widened spreads for affected governments and a widespread economic slowdown, but also increased pressures in interbank and wholesale funding markets. Some US-based banks simultaneously faced declining revenue in European businesses, worsening credit risk from exposures to Euro area borrowers, and increased funding costs. Risk drivers may also be linked to multiple types of exposure across risk categories. For example rising interest rates can drive mark-to-market losses for AFS and HTM portfolios, and greater credit losses on variable rate loans. This driver-based view is much more readily linkable to scenario development, making connections across portfolios much more explicit, increasing transparency and providing linkages within the organization with respect to the risks themselves.

Risk identification cannot be limited to the risk function; the entire organization must be involved

Thirdly, those involved in risk identification and assessment will need a way to communicate (and debate) the significance of the identified risks. Evaluating the relative importance of identified risks and their likelihood of coinciding is critical, in order to focus management attention and resources on the vulnerabilities (or collections of risks) that could most meaningfully threaten the institution. Borrowed from advanced operational risk approaches, some firms have adopted a simple "likelihood versus severity" matrix (see illustration) for this purpose. This framework may apply to granular articulations of the risks within individual business areas as well as more aggregated articulations at the enterprise level. Frameworks such as this allow the organization to maintain a comprehensive list of risk drivers while also helping users focus on those risks relevant for their specific applications.

Exhibit 3: Illustration of risk likelihood vs. impact matrix



Source: Oliver Wyman Analysis

In terms of operational requirements, the first is greater engagement by senior management, business units, and Finance. Senior management has the most holistic view of the institution's risks and risk drivers, enabling them to identify common drivers across risk types, and to know which risks are the most significant. Engagement from senior management is also critical to ensuring that the exercise receives sufficient attention and is more than a regulatory compliance exercise. Meanwhile, risk identification cannot be limited to the risk function. The entire organization must be involved in order to ensure comprehensiveness, including not just balance sheet risks but also risks to future revenue streams. Such broad involvement of the organization will improve understanding of the true sources of risk, clarify how risks relate to specific business activities, and provide the best chances of identifying newly emerging risks.

Documentation and transparency are also critical not just for compliance reasons, but also to ensure the full value is extracted from the process. It is not sufficient if a narrow group of key individuals has a deep understanding of the organization's significant risks but others lack that transparency. In part, risk identification is a process that collects information that is already known by individuals across the organization and packages the often disparate pieces of information in a way that creates transparency around the risks, their key drivers and their approximate magnitude. Detailed documentation of the risks in a consistent risk assessment template (see Exhibit 4) helps to ensure this information can be used for a range of applications by users who otherwise would not have the same comprehensive understanding of the risks.

While risk identification happens organically and continuously throughout the organization, a periodic, formal process is needed to ensure that the full list of risks the institution faces, and the assessment of their magnitude, are up-to-date. The frequency of this formal risk identification process must consider the rate at which risks evolve and the frequency of downstream processes that make use of the information. For many institutions, the full formal process should be conducted no less frequently than annually, but should be updated in the interim as the institution's risk profile changes due to external shocks, potential emerging risks, acquisitions or other factors.

Exhibit 4: Illustration of standardized risk assessment template

A. RISK DEFINITION

Level 1 risk	Level 2 risk	Definition
Credit	Credit concentration – Oil & Gas	Risk that a large number of Oil & Gas exposures default due to a downturn in the sector

B. UNDERLYING DRIVERS

- Direct driver: oil & gas prices
- Indirect drivers: OPEC actions, Middle East conflict, anti-fracking legislation

C. QUANTITATIVE METRICS

Metric	This quarter	Last quarter	Management limit	Board risk appetite limit
Exposure as % of wholesale credit exposure	**4.8%**	**5.1%**	5%	6%

D. QUALITATIVE INFORMATION

- Concentration in sector has decreased due to tighter underwriting criteria and pricing strategy
- Oil prices have now stabilized, though a recovery in prices is not predicted
- Management will continue to reduce concentration in the sector to mitigate risk of further price shocks

E. SIGNIFICANCE ASSESSMENT

	This quarter	Qualitative assessment
Residual likelihood	Annually to 1 in 5 years	Risk could cause significant loss in shareholder value and result in earnings announcement
Residual impact	Severe	
Overall significance assessment:		**High**

F. EMERGING RISK IDENTIFICATION

- Risk is a well-known risk for the bank
- Magnitude is not increasing rapidly
- Therefore, this is not an emerging risk

Source: Oliver Wyman Analysis

COMMON CHALLENGES AND PITFALLS

It is far better to have an imprecise assessment of the size of a risk than to omit a risk due to difficulty in quantification

As institutions upgrade their risk identification processes, there are a number of key challenges observed and anticipated:

- **Achieving organizational engagement**: a robust risk identification process requires broad participation from across the organization. Key stakeholders may be hesitant to participate or honestly identify and assess risks – particularly if they perceive it to be a pure compliance exercise. As indicated above, involving senior management and business units in reviewing, challenging and complementing the risk identification results helps drive personnel to fully engage in the process and ensures that risks are better linked to business activities.
- **Developing a robust assessment framework**: while a single metric for assessing the significance of risks is highly desirable, it is practically difficult. Under the likelihood and severity approach described above, severity can be defined in multiple ways. Some risks – e.g. certain strategic and reputational risks – may be impactful from a long-term economic value perspective but not from a near-term accounting perspective. For other risk types, quantifying the severity may be extremely difficult. Qualitative significance assessment criteria are therefore needed to complement quantitative thresholds to ensure such risks are not missed. It is far better to have an imprecise assessment of the size of a risk than to omit a risk due to difficulty in quantification.
- **Ensuring consistency**: the risk identification process is necessarily very distributed, touching virtually all areas of the institution. Consistency in how risks are defined and assessed is therefore a challenge. An appropriately senior and well-resourced central team should therefore oversee the process and work with key stakeholders to ensure consistency across the organization. Tools such as common risk assessment templates, guidelines for risk identification and assessment, clear and consistent likelihood and impact definitions are also needed to provide additional guidance and to ensure required information is consistently collected.
- **Ensuring comprehensiveness**: ensuring all risks are identified is the core challenge for risk identification. This includes risks outside of the traditional risk types owned by risk departments (e.g. credit, market, operational and liquidity risks) to incorporate revenue, expense and other components impacting financial statements. The design of the process and selection of the participants in the process should take this into account. For example, the use of parallel top-down and bottom-up processes (as depicted in Exhibit 2) provides a higher likelihood of identifying all of the organization's key risks than either process in isolation. A top-down process is led by senior management and should focus on the organization's most important risks, while a bottom-up process is conducted by management across the entire organization, harnessing information already gathered through processes such as the Risk and Control Self-Assessment (RCSA). Comparison of the output of these processes, as well as external views on key and emerging risks, in formal risk identification workshops, is most likely to identify the full suite of the organization's vulnerabilities. Owners of the risk identification process should recognize that the process must encompass the broader organization to achieve comprehensiveness.
- **Considering both position-driven and business activity-driven risks**: institutions often focus on today's exposures as sources of potential loss and risk. This is only part of the set of vulnerabilities. Strategic, business and operating activities also result in structural risks that may be unrelated to today's positions. For example, long-term economic stagnation may lead to low investment and low trading volumes, hurting earnings in sales and trading activities. Other examples of such activity-driven structural risks include reputational events leading to employee or client attrition.

- **Aligning risk identification with Intermediate Holding Company (IHC) scope**: for FBOs in the US, a challenge will be developing a process aligned with the scope of the IHC. This new legal entity structure in most cases does not align with existing management and reporting hierarchies, around which legacy risk assessment approaches have been structured. Furthermore, institutions will need to identify and consider risks arising from their position in a broader international organization – such as risks related to revenue transfer agreements among legal entities.

CONCLUSION

The new paradigm of risk and capital management demands more from the risk identification process. Much of risk management is focused on complex and sophisticated modeling, but ultimately, if the right set of risks is not being considered, and the underlying drivers of these risks are not well understood, the conclusions and action plans drawn will be limited in value. Improved comprehensiveness, wider organizational engagement and increased focus on thoughtful, forward-looking assessment of underlying risk drivers are key elements to upgrading risk identification capabilities and good risk management. Risk managers must design processes tailored for their organization to achieve these requirements. This will be especially important for FBOs as well as institutions with complex or non-traditional profiles entering the US CCAR process for the first time. Many existing CCAR banks also need to upgrade their risk identification processes, while even those who have already invested in upgrading their process need to frequently repeat the process and update their view of risks as the institution's risk profile and market conditions evolve. Only then can risk identification effectively serve scenario design, risk measurement, and broader risk management needs to help financial institutions weather the next storm.

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 or by phone at one of the following locations:

AMERICAS

+1 212 541 8100

EMEA

+44 20 7333 8333

ASIA PACIFIC

+65 6510 9700

ABOUT THE AUTHORS

DOV HASELKORN

Partner in the Americas Finance & Risk and Strategic IT & Operations Practices
dov.haselkorn@oliverwyman.com

ILYA KHAYKIN

Partner in the Americas Finance & Risk Practice
ilya.khaykin@oliverwyman.com

ROSS EATON

Principal in the Americas Finance & Risk Practice
ross.eaton@oliverwyman.com

www.oliverwyman.com

OLIVER WYMAN