Henley Business School
UNIVERSITY OF READING

CAPCO

JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

BUSINESS MODELS

Transforming the theory and practice of risk management in financial enterprises

TOM BUTLER | ROBERT BROOKS

AUTOMATION

Henley Business School – Capco Institute
Paper Series in Financial Services

#46
11.2017

THE HENLEY MBA

Realise your potential with an MBA
from a triple-accredited business school.

hly.ac/the-henley-mba

Henley
Business School
UNIVERSITY OF READING

Where business comes to life

AACSB ACCREDITED

EFMD EQUIS ACCREDITED

ASSOCIATION OF MBAS ACCREDITED

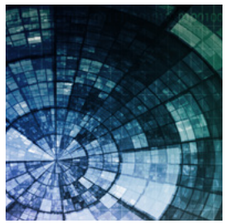
JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

AUTOMATION



BUSINESS MODELS

INVESTMENTS

Transforming the theory and practice of risk management in financial enterprises

TOM BUTLER | Professor, GRC Technology Centre, University College Cork, Ireland
ROBERT BROOKS | Director, Risk Advisory, Deloitte, London, UK

ABSTRACT

This paper highlights the problems facing financial institutions in managing risk at an enterprise level. Chief risk officers (CROs) are confronted with the significant task of managing risk due to the high degree of uncertainty over the provenance and accuracy of risk data and information. This paper, therefore, considers the following questions:

- What is required to provide the group risk function with the same level of oversight and control over risk data and information that enterprise resource planning (ERP) systems have provided group finance?
- What is required for the wholesale transformation of risk management in the enterprise?
- How do business operating models need to change to facilitate true integration of business objectives and related risks?

While the problems with the siloed nature of risk management have been noted, the final point above is concerned with the disconnection between the management of business objectives and that of risk. The fundamental question that this article aims to answer is: How can GRC (governance, risk management, and compliance) practice and systems evolve to support the integration of risk management with business management?

1. INTRODUCTION

The banking industry is, in our opinion, at a cross-roads in terms of how banks address the challenge of navigating between the **Scylla** and **Charybdis** of regulatory compliance and enterprise risk in order to maximize shareholder wealth, while also meeting the expectations and information needs of an increasingly diverse set of stakeholders. We can see from the deluge of fines and other penalties levied by regulators in recent times [CCP (2015)] that some banks appear to be following **Odysseus** in choosing between what they consider to be the lesser of two evils – that is, avoiding grappling with the swirling whirlpool of enterprise risk while navigating the Messinian financial straits.

Yet, others appear to be oscillating between the rock and a hard place in terms of meeting the challenges of regulatory compliance and addressing the complex, paradoxical issue of enterprise risk, without doing either to the satisfaction of regulators or stakeholders. While banks appear to be willing to incur regulatory fines, accepting the recent volatility in global banking stocks is something else altogether, as shareholder wealth is being steadily eroded. Some now argue that the problem of addressing enterprise-wide risk effectively, and with due reference to regulatory requirements, can guarantee safe passage through these dire straits. In navigating this course, it is the visible hand of the CRO that needs to be on the tiller. Thus, it is in the hands of the CRO, as the bank's **First Officer**, that the safety of the financial institution lies in today's uncertain environment [Mikes (2008)]. Indeed, the same could be said of the banking industry, where systemic risk is concerned.

This paper considers the challenges the CRO faces in managing organizational risk in a highly-regulated industry. The management of enterprise risk is a complex activity, and a CRO may be forgiven for envying his fellow C-suite colleagues, whose tasks are not as onerous in informational terms, or equivocal in terms of internal and external expectations. It is significant that while there is "an abundance of principles, guidelines, and standards" and "risk management is a mature discipline with proven unambiguous concepts and tools," Mikes and Kaplan (2015) argue "that risk management approaches are largely unproven and still emerging." This applies, in particular, to the management of enterprise risk. Hence, the challenges facing the CRO are considerable. However, the CRO's role is complicated considerably by the paradox that banks are inherently risk-takers – as risk-taking is an essential part of business activity in financial institutions, more so than any other. In the absence of an enthusiasm for taking risks, the types of rewards valued by stakeholders (including internal actors, such as traders) and shareholders, in particular, will not accrue.

"The management of enterprise risk is a complex activity, and a CRO may be forgiven for envying his fellow C-suite colleagues, whose tasks are not as onerous in informational terms, or equivocal in terms of internal and external expectations."

A riskless bank is a logical contradiction, a dysfunctional institution that will be as doomed to fail as its opposite. The CRO in the riskless bank sees all risks as bad. This is problematic as the baby of good risks is often thrown out with the bathwater of bad risks [Stulz (2015)]. In considering the nascent body of research on such matters, we argue that the role of the CRO is to work with C-suite colleagues to maximize the opportunity for good risk-taking, with profitable outcomes, while minimizing bad risk-taking and associated losses, including regulatory penalties.

2. WHY WE NEED TO RETHINK HOW RISK IS MANAGED IN THE ENTERPRISE

In the 1990s, the finance function in business enterprises underwent a transformation through the adoption of ERP systems, which later became enterprise systems. The business driver for this transformational change was the need to gain control over the finances of large corporations by removing the duplication of effort in financial accounting across business units. Financial and accounting data was, like today's risk data, stored in data silos dispersed across the enterprise. This made the production of enterprise-level financial statements problematic, it also made internal and external auditing extremely difficult. ERP-enabled reengineering and transformation of financial audits considerably enhanced transparency and control of enterprise-wide financial and cost accounting to the chief financial officer (CFO) [Morris (2011), Chang et al. (2014)].

The need to automate the auditing of enterprise risk has driven the management of processes to control

risks within banks. Consider, for example, that controls testing is typically being employed to manage the various categories of operational risk, including IT risk, business resilience, and so on. This has clear efficiency gains for banks that automate and align control processes globally. In this regard, GRC tools are being employed to transform risk management functions and they continue to be invaluable for this purpose. However, there is a realization that financial enterprises need to transcend the process automation perspective and look at the problem of risk management in a different light.

Several questions present themselves for consideration at this point. Why, for example, would one wish to consider risk in an integrated way? What benefit does an integration approach offer, when it is widely accepted that risk management is best carried out by the first line of defense? What are the implications for risk management when, as Argyris (1976) argues, "espoused theory" in an organization is commonly at odds with the "theory in use"?

One "espoused theory" in common currency is that it is the first line of defense, usually operational management, that owns and manages the risks in an enterprise. Consequently, operational managers are accountable for applying corrective actions to address deficiencies in processes and controls [Sadgrove (2016)]. In other words, operational managers are, or are expected to be, responsible for identifying and assessing risks, as well as devising, applying, and supervising effective internal controls, while also ensuring that risk and control procedures are operationalized. In summary, the chief "espoused theory" in business enterprises is that operational managers should identify, assess, control, and mitigate risks in a manner that is consistent with their goals and objectives and those of their organization.

The problem here is that this can only be achieved if the commitments of such managers are aligned with corporate and regulatory objectives. However, when it comes to the first line of defense, "espoused theory" is typically at odds with the "theory in use" [Evans and Quigley (1995)], as the recent Wells Fargo fiasco on cross-selling indicated [Back (2016)]. In March 2017, Toronto Dominion Bank lost over CAD7 billion of its value as news reports revealed how bank employees were under pressure to sell inappropriate products to customers. Interestingly, in a statement that is indicative of a defense of "espouse theory," the bank disputed the reports and stated that "the environment described in the media report is very much at odds with how we run our business, and we don't recognize it from our own perspective, experience or assessments" [CBC News (2017)]. This paper offers theoretical and practical insights into how such problems can be effectively addressed.

2.1 Controllable risks

In delineating our thesis, we first focus on controllable risks that are non-financial in character. In our conceptual schema, a controllable risk has the following attributes:

- It is relevant to the achievement of a business objective.
- It is knowable.
- It is survivable.
- It is capable of being influenced by management action.

Thus, we argue that risk events should be able to bring about a desirable outcome or business objective, otherwise how are they distinguishable from random events? The problem here occurs when managers attempt to consider all possible events that could lead to the non-achievement of a valid business goal or objective, which maximizes shareholder wealth and is compliant with regulatory requirements. Since managers, and in particular senior executives, always operate under incomplete knowledge, their rationality is bounded [Simon (1955)]. Consequently, managers typically "satisfice" and adopt a general risk mitigation strategy of "holding capital" [Altunbas et al. (2007)].

Uncertainty and incomplete knowledge is the reason why risk events are often unrecognized or ignored [Taleb (2005)]. However, it may simply be that managers are not able to identify such events as risks, in which case they are overlooked. Alternatively, if managers increase their knowledge of risks and improve their detection capabilities, risk events can lose their ability to influence business outcomes over time. Of course, risk events must be survivable, if individuals and organizations are to learn from them and prepare for the next occurrence. If risk events are identified but uninfluenceable by management action, then managers either accept the risk or remove the related business objective.

It is logical to conclude that in order to control a risk one must first understand it. Hence, the first and second line of defense in a financial institution need to acquire, manage, and apply knowledge about the

business, its objectives, its environment, and the risk itself. While a business objective can be readily identified and known, information about the risks that threaten the achievement of a business objective, and the risks that the business faces once the objective is finally achieved, is not always readily available. This is, therefore, the principal challenge facing business managers in financial institutions. The following section helps address this problem.

3. RETHINKING HOW WE CONCEPTUALIZE RISK

When it comes to certain categories and sub-categories of risk, there is an important business imperative to manage them, as they tend to be predominantly in the bad risk category. We are not referring to risks that may be good at an individual or a unit level, but bad for the enterprise, as they may collectively exceed its appetite for risk-taking. Examples of such risks are business transactions undertaken by traders to maximize their own returns, but that, as a consequence, place the enterprise at risk. Such matters are equivocal in terms of their acceptance by business, and need to be addressed on an individual basis by managers, or prohibited by business rules. Examples of unqualified bad risks, which may be associated with the principal-agent problem, generally fall into the operational or conduct risk categories [Alexander (2006), Jarrow (2008)].

To be able to manage risk better at the enterprise level we need to reexamine risk in a fundamental way. A central plank of our thesis is that a model of risk, and its categorization, is required that reflects the human and organizational realities of risk management in the enterprise. This is particularly true where operational and conduct risks are concerned in financial enterprises.

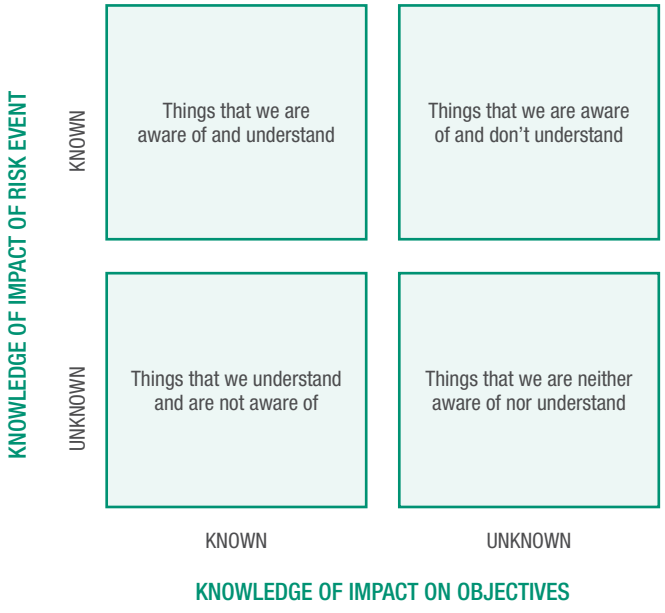
Using the ISO/IEC (2002) guide's definition of risk as our starting point, we conceptualize risk as the "effect of uncertainty on objectives," with the important elements of this definition being "effect," "objectives," "uncertainty," and the 'event' to which we are referring.

- An "event" is the cause that has an "effect."
- "Objectives" are the things that are being impacted.
- "Uncertainty" is the level of (or absence of) prior knowledge – it is not, in this case, an estimate of probability.

"The future is uncertain." While research in quantum mechanics disproved the existence of a deterministic world, some certainties or near certainties about the future in business can, in fact, be deduced. Unplanned events do occur, bringing both good and bad risks with them, and the mere act of planning can uncover the existence of at least some of them. However, successful planning depends, in large part, on the prior knowledge, experience, and expertise of the planner and the complexity ("predictability") of the internal and external environment.

To make our reconceptualization of risk more tractable, we adopt the Johari Window from the field of cognitive psychology [Luft and Ingham (1961)]. This has been used as a tool to enable self-awareness, knowledge, and understanding in several domains, such as in the defense [Petraeus (2015)] and national security sectors in the U.S. (and made famous by Donald J Rumsfeld in his response to the US DoD on Feb 12th 2002) or in thinking about operational risk [Kim (2014)]. Keeping with the Johari Window's 2 x 2 matrix presented in Figure 1, and considering "knowledge of impact of risk event" and "knowledge of impact on objectives" axes, the figure is instructive. Take, for example, the fact that in many organizations risks that can be managed and controlled are often considered to be unmanageable and uncontrollable. Operational and conduct risks, which should be considered known-knowns (KK), and fully managed and controlled, are typically ignored or categorized as either unknown-knowns (UK), known-unknowns (KU), or, worse still, unknown unknowns (UU),

Figure 1: Risk awareness model (RMA)



for a variety of reasons. The primary causes are related to a dearth of information or, rather, the existence of information asymmetries [Abraham and Cox (2007), Liao et al. (2009)].

In order to bring greater clarity to how risk is conceptualized, financial organizations should, in our opinion, conceptualize risks, risk factors, and risk events into four basic categories:

1. UU: these are the risk events that firms do not know about, and only identify them ex-post – these are referred to as "black swans."

2. KU: are risk events that firms know about, but cannot anticipate, understand fully, or quantify.

3. UK: here, the impact on enterprise objectives are known, but the specifics of risk events (because they may be novel in nature) are not known. In addition, because of the siloed nature of financial institutions, or the existence of information asymmetries, such risks cannot be comprehensively quantified at an enterprise level.

4. KK: are risk events that firms know about and where the impact on objectives are fully known, and, therefore, can be quantified, mitigated, or fully eliminated.

Some key conclusions can be drawn from this fundamental analysis:

- Risk cannot be effectively managed without first understanding related objectives. Without a clear understanding of objectives, all events are potentially risk events or, worse still, appear random until the impact is understood ex-post.
- Uncertainty can be reduced by knowing more about the events and their potential impact on objectives.
- There are two controllable elements of risk management that are not generally considered by organizations when managing risk: 1) the setting of objectives; and 2) the acquisition of knowledge about the effect of risk events on objectives, and the potential events that could impact them.
- If individuals are to be responsible for managing risk on behalf of the enterprise, they need to understand how their objectives contribute to the organizational goals.

The implications of this analysis for the CRO and the enterprise risk function are manifold:

- Without a clear link between risk management and the achievement of objectives, too many manageable or controllable risks events are being placed into the UU category and managed by holding capital. The risks in this class should, ideally, be entered under the enterprise "residual risk" category and their consequent impact on objectives entered as "not-known." However, some will be Black Swan events and have significant impact on business objectives.
- Organizational complexity reduces the ability to enforce the link between individual objectives and those of the enterprise, hence events may be known, but their impact on enterprise objectives not known (KU).
- Having a clear understanding of business objectives, and how they cascade down through the organization, means that lead indicators can be created. This means that potential deviations (UK) can be detected and corrected in advance of enterprise objectives being impacted.
- Reducing organizational complexity so that the links between objective, action, and outcome are known (i.e., through process modeling), and potential points of failure monitored for events that could have an impact on objectives, enables organizations to eliminate or mitigate certain risks, such as KK).

Of course, cognition of objectives and related risk events are not necessary and sufficient conditions for a solution to the problem, organizations must apply that knowledge to actively manage/eliminate risk in a routine way.

A review of fintech and Risktech offerings indicate that IT-enabled enterprise risk management solutions are now sufficiently mature, and related technologies available, to permit firms to move from managing risks they consider to be UK, KU, and UU, due to information-related problems, and bring some of them into the KK category.

Taking operational risk as an example, it is evident that because of the complexity and uncertainty in identifying and quantifying risks associated with failed people, processes, and technologies, only a subset of operational risks are being effectively and efficiently managed as KK. This is happening even though it is an endogenous risk category, and the data already is, or can be made easily, available to manage it. With regards to conduct risk, it is evident that many aspects of wholesale, retail, personnel, and third-party conduct risks are manageable as data on risk events, losses, and related factors are available.

Given the recent pronouncements of the Basel Committee on operational risk and the World Economic Forum on conduct risk, firms will have to focus more on managing these two major sources of risk. WEF (2016), for example, states that conduct risk is "likely the largest single source of technologically-driven risk." BIS (2016) advocates a withdrawal of internal modeling for operational risk measurement capital and its replacement with a simplified standardized model. The implication here is that banks will have to adopt more granular and accurate approaches for identifying, classifying, mitigating, and controlling operational risk, if they are to come out on the right side of the proposed "standardized measurement approach." The only confounding issue relates to the presence of qualitative or unstructured data, much of which is the product of subjective human opinion that is open to bias, as indicated below. It only requires that readily available risk management technologies are applied to capture this data and transform it into knowledge, thereby making conduct risks, for example, knowable and actionable. As with operational risk, this is an enterprise-level problem that requires an enterprise-level solution.

4. BASIC PROBLEMS WITH THE CLASSIFICATION OF RISK

There are two schools of thought regarding management of risk in business, with the first viewing risk as being defined independently of business objectives and the second viewing it explicitly in terms of the achievement of organizational objectives [Bromiley et al. (2015)]. When business objectives are expressed quantitatively, such as in financial terms, it is a relatively trivial task to understand the relationships between management objectives at the base of an organizational hierarchy to those at the top. This is because in a quantitative, or financially-based, hierarchy there is a mathematical or formulaic relationship between entities, be it additive, subtractive, multiplicative, or through the application of fixed rules or formulae. Consolidation of the outcomes of business objectives is relatively straightforward, provided the data is available.

In this schema, formalization of organizational structures and processes, and the application of financial or management accounting standards, provide a consistency of classification. For example, profit or

cost centers reflect areas of ownership and control, while business units act as containers of profit centers. In this scenario, if all the known risks in financial statements are controlled, then all that remains are unknown external risks and/or human risks – failed people. The financial audit process, therefore, focuses on the existence and effectiveness of controls and residual risk is the subject of human judgment.

All this stands in stark contrast to the problems posed by risks that cannot be expressed in quantitative terms. Such risks are neither easy to aggregate or disaggregate. This is partly due to the classifications given to such risks, typically operational risks, which give rise to fraud, IT risk, conduct risk, legal risk, and so on.

The current conceptions of operational risk grew around the emergence and practice of risk professions. Thus, labels are accorded to different risk categories and sub-categories in the same way as a biologist might classify different species using taxonomies [Gallagher et al. (2005), Moosa (2007)]. Populating a risk taxonomy by classifying risks is a subjective activity and requires judgment based on a common body of knowledge and understanding within a profession [Blunden and Thirlwell (2012)]. Objectiveness in species classification was not available until the advent of DNA mapping. Objective classification using DNA shows the path and branches of evolution so that species, genus, family, order, class, etc., are accurately classified.

The objective classification of risk in financial services could show how risks are related and permit the identification of the causal chains that give rise to major risks. It could also illustrate where the "gaps" in empirical observations exist; it could also be employed to arbitrate between different subjective judgments or viewpoints.

There have been numerous attempts to classify risks in risk taxonomies. Take, for example, the approach of classifying risks in a taxonomy that disaggregates losses. The problem with this approach is that it is only satisfactory when the business or managerial objective is not to make a monetary loss. The problem with the "loss events" construct is that it is wholly quantitative or financial in nature, even if the loss events are often not modeled as such. In this schema, both cause and effect are typically expressed in financial terms, even though risk events that are not financial in nature may be the trigger for the event. For example, it might be reported that a £100 mln loss in the P&L was "caused" by 100 different loss events of £1 mln. This is probably true from a financial risk perspective (e.g., market, credit risk, etc.), where the efforts to manage the risk can focus on the loss event itself, using hedging or diversification strategies. However, the fact that each loss event is caused by a real event is ignored. This raises the possibility that future real events will not be detected. Managers rely on the assumption that each of these risk events impact the market and that, in aggregate, the impact on the market cannot be known. Where the risk event and the loss event can be linked directly, then attempts to manipulate the causal chain are positively discouraged – particularly when this leads to market abuse or insider trading. The exception to this is the action taken by a central bank in areas of current market manipulation, bond purchasing, and so on.

Where non-financial risk is concerned, active attempts to achieve an objective outcome by preparing ahead of time to prevent deviations from the outcome is the optimal way of managing risk. The only other alternative is to let the risk materialize and remediate it after the event. However, understanding the causal chain is critical, as it will ensure that managers take steps to avoid deviation from the trajectory required to reach intermediate goals and ultimate objectives by preparing for and negating risk events. This, however, is a costly approach to risk management.

The often used and least costly approach is to map the critical path and to design-out potential deviations, or to identify and mitigate locally any detected deviation. However, to be effective, this approach requires detailed process modeling; it also requires a better understanding of the type of risks under consideration [Rosemann and Zur Muehlen (2005)]. There is little evidence that either conditions are being met in practice. We turn next to this topic, which builds on the RMA presented in the previous section.

4.1 Characteristics of knowable and controllable risks

In order to begin to address the above problems with a risk classification approach, we extend the conceptualization of our RMA by defining the characteristics of knowable and controllable risks. First, they are **additive**: examples are accounting risks related to debtors' ledger, creditors' ledger, etc. These are factors that can be measured objectively. Second, they are **auditable**: knowable and controllable risks rely on the "chain of custody" of information to manage them. This approach relies on the fact that there is an

immutable truth at the start of the chain that can be traced to an output, without manipulation on the way. If the entire chain of evidence is within an organization, its validity can be verified. Problems occur, however, when the chain crosses organizational boundaries. Third, **compound** risks are those that are insignificant in relative scale, at the bottom-tier of the organizational hierarchy, but become problematic when they interact with other categories of risks, and exert an enterprise-level effect. Fourth, **singular** risks that impact business objectives to the same extent, wherever they occur in the organization (e.g., reputational risks such as LIBOR manipulation). Such risks are characterized by a separation of the owner of the risk and the actor(s) from which the risk emanates – for example, the LIBOR manipulation resulted in the boards of firms having to take ownership, even though the "causal owner" was much lower in the hierarchy. Fifth, **poolable** risks, such as IT risk, which is a pooled risk as it requires particular levels of expertise across both IT and business functions. Here, managers need to possess specific levels of domain knowledge to understand such risks.

Another category of knowable risks is, in our opinion, neither controllable nor easily detectable. We know they can occur because they have occurred previously, but they are not predictable. Sub-categories here include **internal risks**, such as employee risks, emanating from poor judgment, criminal intent, reckless behaviors, negligence, incompetence, and so on. In addition, there are **external risks**, such as customer risks, where the chain of evidence for audit begins outside of the organization.

Then there are risks that are unknowable due to uncertainty. These usually have an impact on an organizations' **survival objectives**. Such "black swan" risks may lead to the physical cessation of business. Risks in this category include solvency-related risk events that occur when decisions taken inside or outside of the organization have a domino effect and impact on a firm's ability to trade. Such risk events may originate in, for example, a decision to delay payment to creditors, a breach of trust, or reputational damage with stakeholders, and so on. Responses to such risks depend on operational resilience, or reality antifragility, as Taleb (2012) puts it.

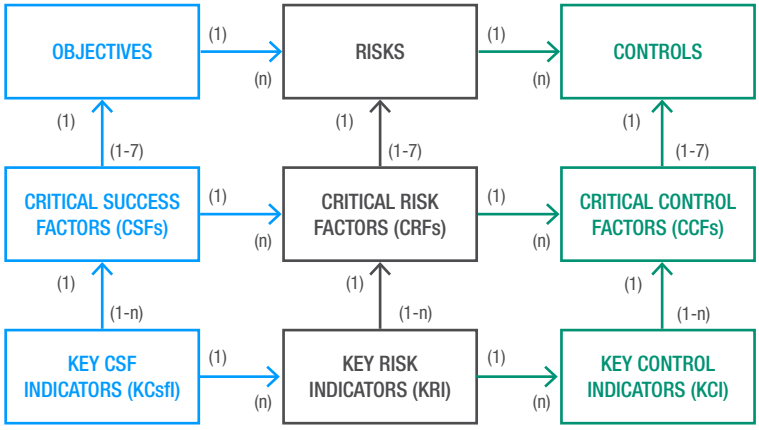
For all these reasons, we argue that financial organizations need to manage risk in the context of business objectives and transcend the tendency to silo risk while also separating and divorcing business and risk management processes. It is to this topic that we now turn.

5. AN INTEGRATIVE APPROACH TO MANAGING BUSINESS OBJECTIVES AND RISKS

Risks at all levels in an enterprise should be linked to the achievement of related organizational objectives. However, there is little guidance in the academic or practitioner literatures on how to achieve this. There are certainly a wealth of complex standards, frameworks, and methodologies that purport to help practitioners manage risk, however, in our opinion, these are either too narrow, too fragmented, or are simply too labyrinthine, resulting in practitioners becoming lost in the detail and failing to realize the benefits. Moreover, none provide the type of informational capabilities to serve as a model for the form of enterprise-wide risk management system required by CROs to serve the information needs of the C-suite or the boards of financial institutions.

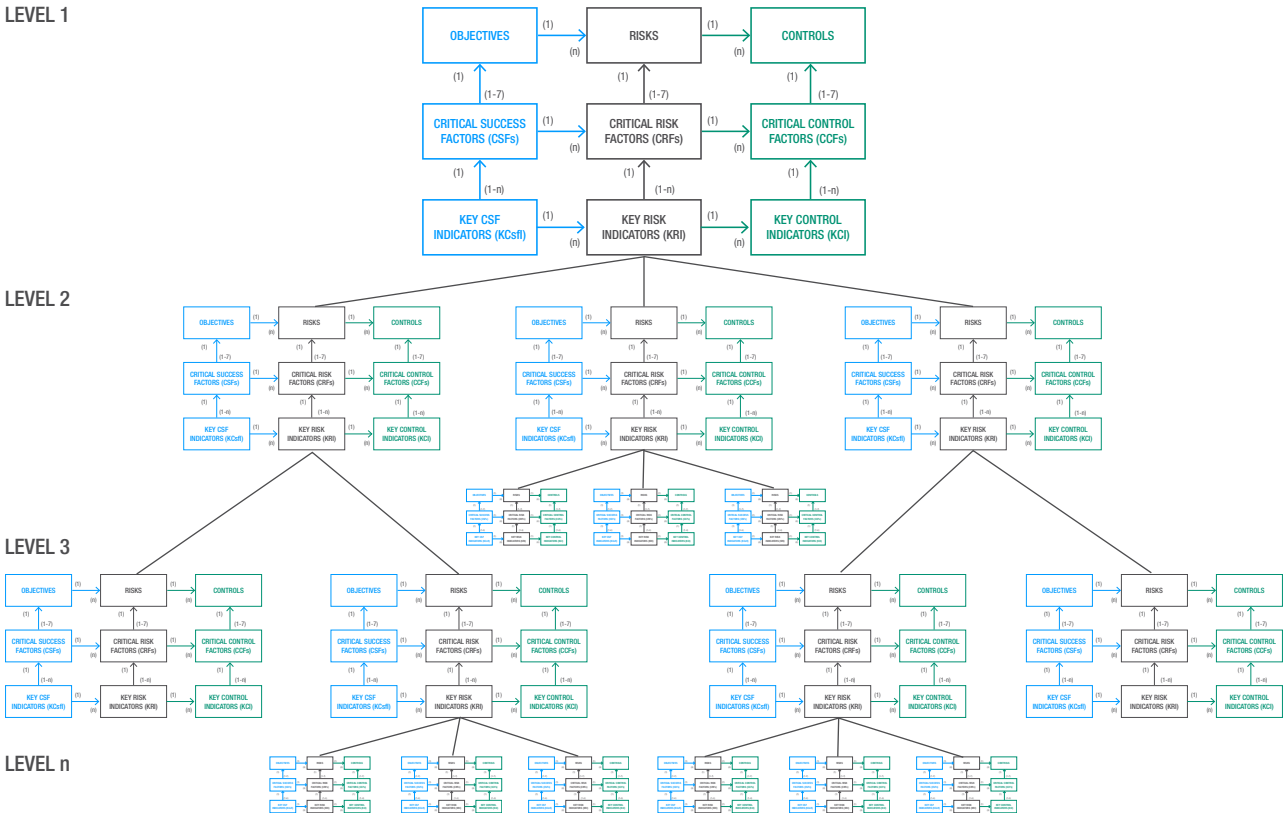
This paper draws on seminal work of Rockart (1979) on

Figure 2: A CSF-based model on linking business objectives, CSFs, risks, and controls



"critical success factors" (CSFs) and Kaplan and Norton (1996) on the "balanced scorecard" to present insights into how all this can be achieved. Figure 1 illustrates our perspective. Rockart (1979) defines critical success factors as "the limited number of areas in which results, if they are satisfactory, will ensure successful competitive performance for the organization. They are the few key areas where "things must go right" for the business to flourish. If the results in these areas are not adequate, the organization's efforts for the period will be less than desired."

Figure 3: Hierarchy of objectives, risks, and controls



CSFs are different from objectives and goals. Objectives are general statements about the directions in which a firm (sub-unit or manager) intends to go, without stating specific targets to be reached at particular points in time. Goals are the specific targets that are intended to be reached at a given point in time by managers. A goal is thus an operational transformation of one or more objectives. Hence, a manager's goals are the targets that they will aim for.

CSFs are the key areas of activity that most influence success or failure in their pursuit of goals and related objectives. A CSF is what has to be done in order to achieve a particular goal and a related objective. Goals and objectives are the ends, while CSFs are the means to those ends. Figure 2 illustrates this relationship graphically. However, it is clear from the literature that the CSFs-goals-objectives construct is rarely adhered to. For simplicity's sake, we conflate goals and objectives to simply objectives, as indicated in Figure 1. Following Rockart, our schema posits that each objective has 1-7 related CSFs. Likewise, each CSF has 1-n key indicators. Mapping this schema onto the risks and controls dimensions results in similar cardinalities. It is clear that each objective may have 1 or more (n) risks, while each risk may have 1-n controls. This type of relationship also exists at the critical factors and key indicators levels, as indicated in Figure 2.

In Rockart's schema, CSFs and objectives are influenced by "problems" – i.e., business problems to be solved. Attaining business objectives involve undertaking risks. From a risk management perspective, this indicates the existence of "critical risk factors" (CRF), the presence of which influence the attainment of CSFs. We also believe that just as CSFs may be decomposed into measures, such as "key CSF indicators" (KCsfI), CRFs may be decomposed into measures such as "key risk indicators." Usually, the intermediate modeling of CRFs is omitted with risks simply being mapped to KRIs. This omits an important analytical step, which could result in the omission of important risk indicators and poor measurement of risks. It is also clear that there may be relationships and overlaps between both sets of measures. Extending this model to include controls, we posit the existence of "critical control factors," which

are decomposed into "key control indicators" (KCIs). Unlike KPIs, KCsfIs, KRIs, and KCIs are lead indicators and, therefore, more relevant to the task at hand.

Figure 2, therefore, presents a normative, parsimonious model that captures the essence of how risks should be managed by business managers in the first line of defense. This approach of defining objectives, in terms of the CSFs that are required to meet them, in concert with the CRFs that impact the attainment of CSFs, and the controls required to mitigate risk events, appears to be a common-sense approach. This stands in contrast to the business as usual approach, where first line operational managers fail to identify, assess, control, and mitigate risks in a manner that is consistent with their objectives and those of their organization. Then, there are the risk and control frameworks and methodologies that purport to help practitioners, but are difficult to implement due to their complexity or ability to scale horizontally or vertically. Our research indicates that objectives and CSFs cascade in a hierarchy from top management down, while also spanning organizational units and functions.

Figure 3 illustrates the scalability of the proposed model, which incorporates qualitative and quantitative data. It is important that if this model is to be enabled by appropriate technologies, then it could provide both roll-up and drill-down capabilities, enabling risk data aggregation and enhanced risk management capabilities.

6. RISK MANAGEMENT AS DOUBLE LOOP LEARNING

Argyris (1976) argues that organizations typically engage in "single-loop learning," in that they generally apply fixed models for decision-making and problem-solving. In general, organizations rarely go beyond single-loop learning as a mode of behavior because they fail to question the assumptions underpinning their strategies or decision-making routines. Hence, they fail to develop what Aristotle calls practical or experiential knowledge. They also fail to build or evolve technical knowledge and skills. All this condemns organizations to apply the same decision-making and problem-solving routines over and over without learning how to improve their knowledge. This is a critical issue. Omerod (2007) illustrates that success in any area of endeavor is elusive because it is dependent on possessing appropriate knowledge about the organization, its business, and related risks. To achieve this, Argyris (1976) argues that organizations need to engage in "double-loop learning." This involves critical sense-making and subjecting governing assumptions and beliefs to question, the answers to which point to the need for new decision rules and the development of new routines. However, organizations also need to practice knowledge sharing, bridge knowledge gaps, and making learning outcomes explicit. We now consider this in the context of organizational knowledge and capabilities, and the management of business objectives.

The evolution of risk management with respect to business objectives depends on learning and knowledge acquisition. Knowledge of how to achieve an objective is related to the definition of CSFs for its attainment. However, we argue that there is also a need to identify CRFs in order to implement controls so as to ensure that the objectives-CSFs along the critical path are realized. It is important to understand objectives in terms of what is required to achieve them – i.e., CSFs and CRFs – otherwise actors are continuously confronted by decisions to consider all options over a range of paths in order to identify the next move.

Decision-making under uncertainty, caused by a failure to prepare, adds unnecessary complexity. The quality of the decision is a function of an agent's commitments, experiential knowledge, capabilities, intent, objectives, and a web of social and cultural conditions and factors [Nelson and Katzenstein (2014)]. However, as indicated above, managers typically "satisfice" on bounded knowledge and rationality [Kahneman (2003)]. If time and resources permit, managers may enact their decision theories through risk scenarios using focus groups, on one hand, or predictive modeling or simulation, on the other [Blunden and Thirlwell (2012)].

The research cited herein indicates that managers' decisions are typically based on experiential knowledge of critical success or risk factors expressed in the form of heuristics or routine decision patterns [Busenitz and Barney (1997)]. This offers a quicker route to the achievement of an objective. Typically, a manager defines a critical path, intermediate objectives, and then manages the deviations from these. Project management typically relies on such techniques. This requires effort and judgment to determine whether a deviation has occurred, and put a corrective action in place. Human judgement is augmented as the trajectory to the objective becomes known (estimated in reality). However, there is a need to focus on risk factors and

events that change the trajectory.

A **controllable risk approach** is possible through enhance learning and the development of new decision-making routines. In the proposed schema, all potential points of deviation from intermediate CSFs-objectives can be mapped and measured, and controls put in place to detect and correct deviations. Our model above also indicates a need to identify and measure CCFs as well as CRFs. This approach helps reduce the amount of human judgement required by adopting a "rule-based" approach to decision-making. Automated controls may then be employed for potential points of failure, as uncertainty and decision complexity is lowered.

7. ENTERPRISE INTEGRATION OF OBJECTIVE MANAGEMENT AND RISK MANAGEMENT

The optimal "risk appetite" models for operational risk tend to follow Kaplan and Norton's (1996) "balanced scorecard" approach. Here, the categories in the scorecard align to the objectives of the organization, they are (or should be, if the user is faithful to the model) linked to the CSFs for achieving them, and related measures are identified and operationalized. However, this is not the norm. In addition, organizations, whether they use the balanced scorecard or not, typically create a risk taxonomy that stands separate from, and is not integrated with, organizational strategies or objectives, if they are indeed defined and codified.

This paper argues that organizations should be developing and managing a taxonomy(ies) of business objectives that are integrated with risk and control taxonomies. In this scheme of things, the macro objectives are expressed in a taxonomic hierarchy, different levels and branches of which are owned by appropriate managers and units within the organization. Based on research and practice, we now briefly examine a general framework of business objectives using a basic taxonomy.

Enterprise risks are those events that impact the upper levels of the objectives hierarchy presented below. Addressing such risks are influenced by organizational knowledge and capabilities.

Level 1: Survival objectives

- License for business and trading.
- Ability to trade (sell).
- Ability to buy inputs (buy).
- Ability to staff.
- Ability to direct and coordinate resources.
- Resilient to external events.

Level 2: Strategic objectives

- Ability to satisfy stakeholders (valuation, profit motive).
- Financial integrity.
- Solvency.

Level 1 and 2 capture an organization's survival and strategic objectives. The subsequent levels in the objectives taxonomy should map to the organizational structure (extending the levels already described).

Objective and risk decision-making on more strategic and tactical objectives will clearly be the province of higher levels in the organizational hierarchy. And where knowledge and expertise to inform decision-making exists elsewhere in the organization, sufficient governance needs to be put in place so that the owner of the objective is responsible and accountable for decisions.

Assuming that an enterprise risk management system exists to manage objectives (according to the model in Figures 2 and 3, for example), what supporting roles would such a system be expected to perform? We argue that an enterprise risk management system should:

- Provide the integrative capabilities for managers at all levels to define their objectives, CSFs, and associated measures.
- Identify the related risk events and map these to CRFs and measures.
- Monitor and manage the taxonomy of objectives and map them to the correct risk nodes in the hierarchy.
- Define controls for risks, and CCFs with associated measures where appropriate.
- Confirm that controllable risks are controlled, and that the control environment is heathy.
- Provide assurance that:
  - Decision making is made at the right level of the organization.
  - Good decisions are being made.
  - Bad decisions being made as a result of incorrect information is eradicated.

- Minimize the existence of compound risks.
- Monitor the existence of singular risks and ensure that correct governance is in place for them.
- Provide internal audit capabilities that monitors the "healthiness" of the pooled risk.
- Provide a heatmap/dashboard to the C-suite and board indicating the levels of risk resilience.

8. ON THE RELATIVE INFANCY AND IMMATURITY OF ENTERPRISE INFORMATION SYSTEMS FOR RISK MANAGEMENT

It is clear that the chief risk executive of any bank is the CEO, not the CRO [Stulz (2015)]. The CEO of a financial institution with an appropriate risk culture will, however, value and leverage the particular knowledge and expertise of the CRO. Thus, research has indicated the importance of the relationship between the CRO and the CEO, and as the findings presented above illustrate, as far as enterprise risk is concerned CEOs need to listen to their CROs. Stanton (2012), who participated in the U.S. Financial Crisis Inquiry Commission (FCIC), found that the presence of "constructive dialogue" in a bank, and the inclusion of the CRO and risk perspectives in decision-making, was characteristic of those banks that avoided the type of losses that occurred in distressed or failed banks in the financial crisis.

Stanton (2012) argues that engaging in constructive dialogue will help empower CROs and the risk function to create the institutional framework – consisting of regulative, normative, and cultural dimensions and mechanisms – required to make the commitment to enterprise-wide management of risk a reality [Brandes et al. (2005)]. It is important to note that while the CRO and the risk team are responsible for identifying, quantifying, monitoring, and controlling risks, it is, as indicated, the function of the business to actually manage risks at operational, tactical, and strategic levels. Nevertheless, it is the responsibility of the CRO and the risk function to collaborate with the business to develop strategies, practices, and routines that are risk-optimal in terms of their profitability and contribution to shareholder wealth. Thus, the CRO has to balance the need to be objective and independent, with the requirement to collaborate with the business. To be a credible agent for change across the enterprise, it is vital for the risk function to be adequately informed, and it is here that information technology is, and will increasingly be, a vital source of hard data,

business intelligence, and management information. Unfortunately, the CRO and the risk function are not as well-served in this regard as other colleagues in the C-suite, such as the COO or the CFO.

8.1 Problems with information systems' support for the risk function

Financial, accounting, and transaction processing information systems in banks are highly mature in terms of their support for information and decision-making in the disciplines of finance and management. Such systems also help automate and enable reporting according to accepted standards, such as GAAP and IFRS. Thus, the CFO typically has at their fingertips the ability to determine the provenance of financial data and information through all levels and across functions in a bank – retail, commercial, or investment. The CRO is not as well-endowed, in terms of informational resources, as the CFO, as IT-enabled enterprise risk management systems are extremely immature, and comprehensive enterprise-level dashboard capabilities practically non-existent. Direct support for this contention comes from the Basel Committee on Banking Supervision's BCBS 239 principles for risk data aggregation [Grody and Hughes (2016)]. There are several reasons for this, which are worthy of reflection.

8.2 Problems of risk data completeness, accuracy, and quality

There is evidence that IT-enabled risk information systems are limited in a number of ways, particularly in terms of support for real-time risk measurement, monitoring, and control. Certainly, real-time risk measures exist for certain activities, but these tend to be silo-based. There is, unfortunately, a bigger problem. As risk management functions have evolved in banks, in particular lines of business and across the industry, areas of specialization have grown around the various categories of risk. This has led to fragmented risk management practices in terms of the application of approaches, capabilities, knowledge, procedures, and, of course, the manner in which risk data is managed and stored. Most significantly, the growth of banks and the digitalization of business has resulted in a proliferation of data silos. Thus, the data required to identify, monitor, and manage risk within and across business lines is stored in the databases of many hundreds of operational systems. The growth of this data is exponential, with new systems being introduced as banks digitalize their business [Tett (2010)].

Depending on the degree of autonomy in each business area within a bank's functional areas, risk executives typically employ unintegrated point solutions (often based on Excel spreadsheets) or risk management software applications developed by the IT functions in-house, or solutions from a range of vendors. However, the overall impact of often ad-hoc, unintegrated risk management systems at an enterprise level is for all intents and purposes negligible, due to their fragmented and siloed nature. In addition, there is an absence of agreed business vocabularies across many financial enterprises. Thus, business objects have multiple data representations, and data has multiple meanings attributed to them. Regulators find this situation extremely problematic.

> "Organizations should be developing and managing a taxonomy(ies) of business objectives that are integrated with risk and control taxonomies."

As a consequence of this, existing risk management systems also contribute to heightened operational risks, as business, IT, and risk professionals manually disambiguate, collate, and analyze business and related risk data. In situations where business lines have created data warehouses or data marts, and more recently data lakes, banks still find that the data is incomplete and unintegrated with key internal and external data. Consequently, accurate, consolidated measures of risk are rarely available for the entire bank or financial organization. Worse still, the provenance of data is problematic due to the manner in which data is governed by business and IT functions [Soares (2015)]. Thus, the CRO and business executives have problems in proving adequate data quality, lineage, and provenance to auditors and regulators, increasing regulatory risk and resulting in greater capital allocations.

8.3 Problems with risk models

The business assumption regarding the accuracy of existing tools and techniques for the identification and measurement of risk is, according to leading academics and practitioners, erroneous [Shojai and Feiger (2010)]. To illustrate this point let us examine the use of value-at-risk (VaR) as an enterprise tool for risk management. The first point to note, however, is that the data on

which VaR models are based must be of high quality, complete, and accurate, otherwise no matter how good the models are, they will produce inaccurate estimates.

VaR is used to measure a variety of risks, from an individual trading desk, to a business line, and on to a measure of corporate risk to be used by a CRO. However, there are significant limitations in using this approach. Building from a VaR for a particular unit or function, multiple VaRs may be combined to develop an enterprise-wide VaR for a bank. Correlations between the risks generated by different units may also calculated. Thus, it is possible, at least in theory, to estimate an overall measure of risk in a bank and to identify areas where risk appetite has been exceeded. In practice, however, there are problems in that VaR cannot be used to measure every risk and VaR models carry significant risks in themselves. Even when different categories and sub-categories of risks can be estimated using VaR, along with their correlations, a true measure of enterprise risk is not possible, as certain risks are not included and correlations estimated [Bamberger (2010)].

8.4 Fundamental behavioral and cultural issues

Then there are a range of more fundamental issues. We know from the work of Daniel Kahneman and others in the field of behavioral finance and psychology that economic actors operate under the influence of a raft of biases, which influence how they perceive risk. Such biases are difficult to identify and contaminate risk models generally assumed to be sound. Other biases and contaminants originate in the existence of competing commitments and moral hazard, where actors are incentivized to act in their own interest or short-term objectives, as opposed to that of their business unit or enterprise [Kegan and Lahey (2001)]. Then there is the nebulous matter of the culture of the bank or institution, which is extremely resistant to estimation or quantification, as are the mountains of qualitative or unstructured data collected and stored in a myriad of data repositories.

As indicated, the origins and emphasis of BCBS 239 reflects the current poor state of enterprise risk management across the industry, as risk data aggregation is, with few exceptions, wholly inadequate. Its principles provide a foundation on which the governance of risk in a banking enterprise can be based. Practitioners note that BCBS 239 does not require common risk metrics and challenge this notion by arguing that risk officers, business managers, and accountants need to architect finance and risk systems that are integrated and possess a common control and reporting framework. Be that as it may, the range of issues outlined above bear witness to the apparent intractability of the problems facing CROs in enabling the management of risk in and across the enterprise. The following section offers some direction in transitioning to next generation financial services.

9. NEXT GENERATION RISK MANAGEMENT IN BANKING

It could be concluded from the above that a CRO needs to possess similar strategic capabilities as those of a CEO, to understand regulations like a CLO, to know the business operations as well as a COO, to navigate financial risk similar to a CFO, to exhibit the same technical knowledge as a CIO, and understand risk data at the level of a CDO. Of course, if other C-level executives could view their business through the eyes of a CRO, then this would help simplify the organizational change that is required in the coming years.

We believe that financial institutions that do not recognize these basic realities will end up in deeper trouble than that which some of the major banks find themselves in at present. With traditional business models under pressure from new entrants and innovations from the fintech sector, and with margins squeezed from all sides, including regulatory compliance, banks will have no option but to take even greater risks. The CRO will make the difference here by enabling the business to identify and maximize the return on good risks and controlling, mitigating, or eliminating bad risks.

Given the regulatory forces and business drivers that currently shape their environment, financial institutions will need to rethink and transform not only their risk functions, but the status and role of the CRO. CEOs need to reorient their C-level teams to accept the risk function as a core business partner, and the CRO as business risk leader, if they are to transform and prepare their banks to face not only current challenges, but the all too certain future challenges and make their banks, as Nassim Taleb would say, “antifragile.” Information technology’s ability to transform organizations by automating their business process and informating

their people is a key enabler here [Zuboff (1991)].

9.1 INFORMATING AND AUTOMATING BUSINESS PROCESSES

Banks are no strangers to the transformational power of IT. IT-enabled software applications are being used to automate risky business processes, such as client on-boarding, KYC, and other customer-facing activities. Innovations in the fintech and regtech sector offer enhanced capabilities to informate and automate their activities across business lines. Digital innovations in e-banking/online/mobile banking, and so on, provide new avenues for automation and elimination of operational risks, such as failed people in anti-money laundering (AML). Utilities and regtech vendors offer a range of services to banks that can augment or replace inefficient and risky operations with tried and tested solutions, with, surprisingly, the support of regulators. Artificial intelligence [Castelli et al. (2016)], machine learning, blockchain [Jessel and Marshall (2016)], and robotics [Cocca (2016), Arwas and Soleil (2016)] are the new buzz words in an industry that is planning to automate, with virtual robots, certain middle and backoffice functions.

These are examples of the use of IT to minimize the need for manual processes across business activities and lines across the organization. Bad non-financial risks, such as operational risks, can be reduced or eliminated by simplifying, standardizing, and automating business processes, particularly where customers or partners in service delivery are concerned. Big data technologies are being used in concert with semantic technologies, predictive analytics, and machine learning to address a range of operational risks, from fraud, to insider threats, front running, and so on. Regtech-based semantic technologies are also being used to help legal, risk, and compliance teams deal with the mountain and complexity of regulations.

9.2 Navigating the digital labyrinth to manage and report on enterprise risk

As indicated, the core of many of the problems banks face in managing risk across the enterprise is the manner in which they manage data; both structured data isolated in siloed databases and spreadsheets, and unstructured data in documents and text fields. With few exceptions across the industry, this approach has seen little change since 2008. As indicated, BCBS 239 is heralding in a new era for risk data governance and risk data aggregation in banks large and small. The financial services industry generates more data and spends more on its storage than any other. Surprisingly,

there persists a basic inability to govern and manage that data, to interconnect it, link it with external information, and to make inferences from disparate and diverse data, wherever it exists. This makes risk management and compliance reporting hugely problematic and expensive. Manual data collation and integration remains the norm across the industry. This generally remains true for the global systemically important banks (G-SIBs).

The Enterprise Data Management Council (EDM Council) stated that the core problem was the absence of a common language or vocabulary within and across banks to describe the business meaning of data and metadata. The EDM Council is a global association of leading financial services organizations, technology vendors, and government agencies based in the US and Canada. The Council recognizes that a common language, enabled by semantic technologies, is required to better manage not only the mountains of data in and across banks, but also manage financial and systemic risks, and to enable comprehensive compliance reporting in the face of increased regulation. Thus, the EDM Council "co-opted" the software industry standards body, the Object Management Group (OMG), to collaborate in the development of, and to help institute, a standard vocabulary called the Financial Industry Business Ontology (FIBO) [Bennett (2013)]. While this is significant development at an industry level, individual banks need to develop related common languages to help add business meanings to, disambiguate, integrate, and link data internally and externally, be it structured or unstructured. Consequently, banks need to address what is the core problem for them and the industry: the absence of a common language to describe both business objects and processes and the risks attached to them. Since these are increasingly digitized, this means developing a common language for their data; one that bridges both business and IT functions of this data. There is also a need to arrive at agreed conceptions of the risks they face, that would, in turn, enable data integration and make risk data aggregation a reality. Thus, there is a need for a related common language for risk, expressed as risk taxonomies that are semantically enriched.

With few exceptions, the current fragmented offerings from the fintech sector are merely adding to the digital labyrinth, as new structured and unstructured data silos are being created. The same can be said of the budding regtech and risktech sectors in terms of offering comprehensive solutions for the particular problems faced by the financial services industry. In solving one problem, eliminating risk through process automation, others may be created.

The solution to the problem of what is a digital labyrinth is technically feasible and practically possible, given the rise of NoSQL technologies [McCreary and Kelly (2013)]. Unfortunately, there are few players in the market providing comprehensive solutions for the industry. One approach that is receiving much attention is data virtualization. This approach provides access to data directly from one or more disparate data sources, without physically moving the data, and presenting it in a form that makes the technical complexity transparent to the end-user. There is broad agreement across industry sectors that semantic metadata (based on the aforementioned common language) is required to make data virtualization and other NoSQL approaches work. Thus, semantically-enabled data virtualization will help underpin both enterprise risk management and enterprise risk reporting.

10. DISCUSSION AND CONCLUSIONS

In reflecting on the challenges facing CROs, we must return to the past to solve today's problems. As indicated, CSFs are those few things that must go well for an individual or an organization to ensure success in a business undertaking. We believe that the CSF method offers a tried and tested approach to rethinking how risk is managed at an enterprise level.

CROs and their risk teams would benefit in applying this tried and tested approach to identify their objectives, CRFs, and related data needs and information requirements. This seems sensible as complexity and uncertainty is the norm and the chances of developing an enterprise-wide risk dashboard remote if fundamental information needs are not formally defined and recorded. It would, for example, help CROs and their teams communicate their information needs to CIO/CTO/CDOs and the business. This is particularly important as information technology, be it fintech, regtech, or risktech, is being harnessed in an ad-hoc manner, with disintermediation of information by multiple systems adding to complexity and opacity of risk data in the CRO's office.

However, we need to go beyond current siloed approaches and apply the same methodology across the enterprise to help executive and managers at all levels, particularly those in the first line of defense, to create an

organizational taxonomy of business objectives, goals, CSFs, CRFs, and CCFs related measures. This should then be mapped to the standard risk taxonomies.

10.1 Reconsidering risk

Effectively managing risk still means we have risk. So, what is risk? What are the characteristics of risks, and why do we care about them? To recap, one cannot have risk without first having an objective to pursue. A risk is an event that may occur to prevent a business manager from achieving a particular objective. An objective could be something as general as being accepted by colleagues, or as specific as making profit on a derivatives deal. At an organizational level, objectives can either be considered as the aggregate of all of the objectives of the employees of the company, or employee objectives being a sub-categories of the objectives articulated by the executive committee.

In the finance function, the fact that objectives can be expressed in numerical terms means that the aggregation of financial objectives is achievable; objectives can be cascaded from top to bottom and activities, actions, and outcomes can be collated and aggregated in the same manner. Even large organizations can ensure that financial objectives are harmonized by using tools such as Finance ERP or modules in Enterprise Systems. As we stated above, problems occur when objectives cannot be expressed in numbers, or when nonfinancial conditions are imposed on those numbers – e.g., rules such as: "must not be from the proceeds of crime," "must not be from money launderers," and so on. The collective term for this type of risk is nonfinancial risk."

"Non-financial risk" (NFR) covers topics as diverse of reputational risk, cyber risk, compliance risk, operational risk, conduct risk, and legal risk. Each risk event may give rise to a loss event, but the risk itself does not represent a financial loss, unlike a market or credit risk. What is true of all NFRs is that if one prevents the risk event, the loss event is also prevented. What is also true of some NFR events is that if one can detect the risk event, one may avoid the loss. Which leads to the (not so) startling realization that the more one knows, the more time one has to prepare, and the more effective one is at preparing, the more likely it is that one will achieve the desired objectives. Thus, the significance of the points made previously for the need to develop double-loop learning.

10.2 How does GRC practice need to evolve?

We believe that the focal point for GRC practice needs to shift from the "risk category" perspective, that is a functional and departmental view of risk, and to align this with an enterprise-wide objectives-driven view. As the CSF-based model above demonstrates, the objectives-driven view is hierarchical and cross-functional in essence. In a business enterprise, upper nodes of the objectives hierarchy tend to be aligned with "survival" imperatives for the organization as a whole, followed by strategic objectives for the enterprise at Level 2, and so on. Hence, business objectives are cascaded or nested from top to bottom of the organization, across business lines and functional units.

> "The core of many of the problems banks face in managing risk across the enterprise is the manner in which they manage data; both structured data isolated in siloed databases and spreadsheets, and unstructured data in documents and text fields."

The current taxonomic or categorical view of risk in organizations is still important, as it represents a pooled area of valuable capabilities. However, once a risk has been identified, its importance or impact should be gauged by understanding where in the hierarchy of business objectives the impact of the risk lies. In addition, ownership of an objective should drive the focus on, or conception of, particular risks within the organization. It is also clear that where a risk that is known, controllable, but currently unmanaged, and which is identified as impacting on nodes in an upper hierarchy, should appear in a related continuous improvement log.

In this scheme of things, risk ratings are considered as objective measures. A risk with a high rating means that it has a singular impact on the related objective or node; a "medium" rating indicates that one or more risks in adjacent objective-risk nodes need to activate before impacting the upper level node; and a "low" rating means that all of the adjacent sibling nodes are required to activate before impacting on the objective-risk nodes at the next level above. Harmonization between risk categories should, however, be automatic, as risks that impact higher objectives rank higher than

those that rank lower.

We believe that risk classifications should, ideally, be system theory-focused. That said, some risks are "singular" in that if they crystalize they will impact the organization as a whole (e.g., regulatory fines for misconduct). Alternatively, some risks that occur lower in the risk hierarchy impact higher nodes (e.g., regulatory risk related to SOX, where, for example, it is assumed that managers take responsibility for the actions of staff). In addition, our proposed schema holds that uncontrolled risks at the bottom of the organization can have a compound impact at the top. Thus, risks need to be identified and controlled at greater levels of granularity.

This brings us to the fact that relevant decisions should be managed by the owners of business objectives. Risk mitigation should be dealt with on the intersection of objective – risk axis, as our model above indicates. The articulation of CSFs and related CRFs should help the design and implementation of related controls and to enable control testing. We have previously indicated that the model can also enable double-loop learning and enhanced decision-making. Thus, the application of our model will help to mitigate those risks caused by decision routines based on single-loop learning. However, we also note that other factors also influence risk decisions as decision makers often:

- Do not own the decision.
- Suffer from a raft of biases.
- Lack knowledge, skills, and capabilities.
- Have poor information and decision support.
- Are motivated to make the sub-optimal or incurred decision (e.g., through incentives).
- Are not motivated to take risk into consideration (i.e., are reckless).
- Make bad decisions deliberately (e.g., engage in misconduct or fraud).
- Make errors or are just negligent.

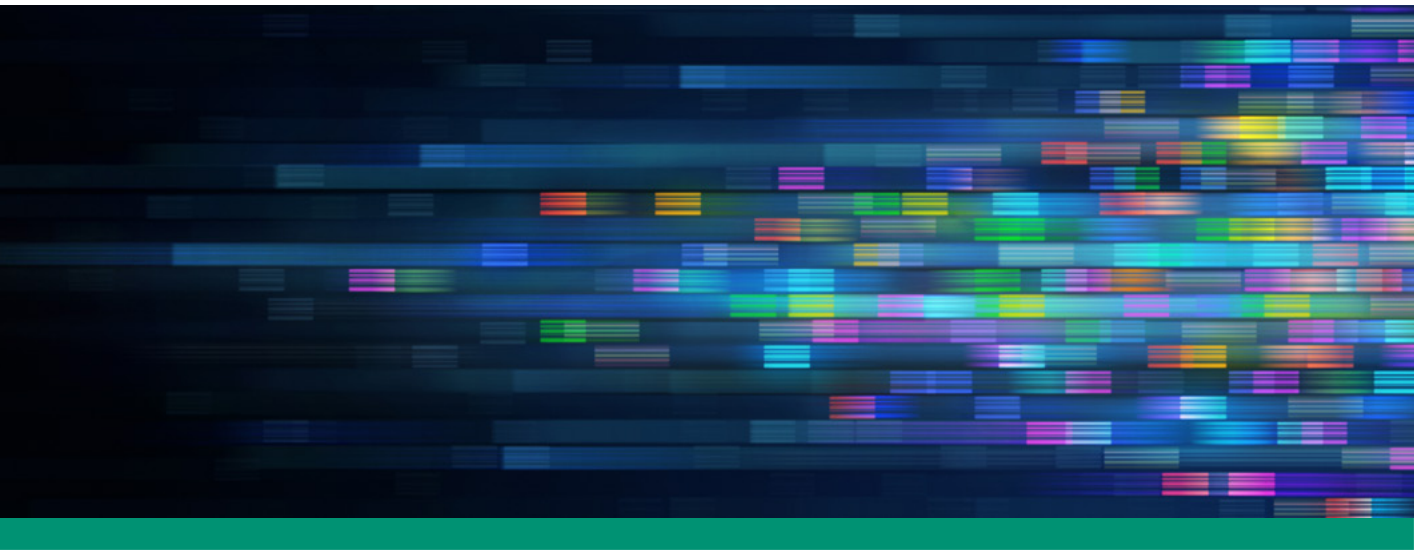
One of the key factors here is the value of information and IT-based system support to address what are basically information-related problems, be they information asymmetries or inability to access information within an organization.

10.3 The future of information systems support for enterprise risk management

The relative comfort the CFO faces in managing enterprise-wide financial data was noted, as was the importance of standards in communicating information and data. An integrative approach to identifying and categorizing objectives, risks, and controls with related critical factors and indicators provides a model for financial services organizations, as well as fintech or risktech vendors, to develop enterprise risk management systems that emulate financial information and enterprise systems.

It is clear that a riskless bank is a logical contradiction. Financial institutions take risks whenever they issue credit or trade in the markets. Such risks are financial and have both an upside and a downside; they are, therefore, undertaken in accordance with an institution's risk appetite. Non-financial risks have no upside and are all downside. Again, risk appetite and business impact of a risk event are the deciding factors. A bank, therefore, needs to be able to identify and distinguish between good and bad risks, in the context of financial and non-financial risks. These simple dichotomies could be used by a CRO and an enterprise risk team to frame their dialogue on risk with the business. Due to the siloed nature of the business and risk functions, as first and second lines of defense, communication is vital, and how such communication is framed is important. We have asserted, based on recent empirical evidence, that if the CRO and their team are not engaging in, or are not being included in, constructive dialogue with the business, then there are significant problems with risk culture in that institution.

We hold that the models we propose in this paper not only help address the good risk/bad risk problem, they also facilitate constructive dialogues at all levels within an organization. Hence, whether they are embedded in an enterprise risk management system or not, they are of material benefit to managers in creating the circumstances where such dialogues take place, with positive outcomes for the organization as a whole.



References

Abraham, S., and P. Cox, 2007, "Analysing the determinants of narrative risk information in UK FTSE 100 annual reports," British Accounting Review 39:3, 227-248

Alexander, K., 2006, "Corporate governance and banks: the role of regulation in reducing the principal-agent problem," Journal of Banking Regulation 7:1-2, 17-40

Altunbas, Y., S. Carbo, E. P. Gardener, and P. Molyneux, 2007, "Examining the relationships between capital, risk and efficiency in European banking," European Financial Management 13:1, 49-70

Argyris, C., 1976, "Single-loop and double-loop models in research on decision making," Administrative Science Quarterly 21:3, 363-375

Arwas, A., and K. Soleil, 2016, "Robo-Advice 2.0: the next generation," Journal of Financial Transformation 43, 30-36

Back, A., 2016, "Wells Fargo's questionable cross-selling strategy," Wall Street Journal, September 9, http://on.wsj.com/2uSSKNW

Bamberger, K. A., 2010, "Technologies of compliance: risk and regulation in a digital age," Texas Law Review 88, 670–739

Bennett, M., 2013, "The financial industry business ontology: best practice for big data," Journal of Banking Regulation 14:3-4, 3-4

BIS, 2016, "Standardized measurement approach for operational risk - consultative document," Bank for International Settlements, http://bit.ly/1nTDSai

Blunden, T., and J. Thirlwell, 2012, Mastering operational risk, Pearson Education Limited

Brandes, P., R. Dharwadkar, and D. Das, 2005, "Understanding the rise and fall of stock options compensation: taking principal–agent conflicts to the institutional (battle) field," Human Resource Management Review 15:2, 97-118

Bromiley, P., M. McShane, A. Nair, and E. Rustambekov, 2015, "Enterprise risk management: review, critique, and research directions," Long Range Planning 48:4, 265-276

Busenitz, L. W., and J. B. Barney, 1997, "Differences between entrepreneurs and managers in large organizations: biases and heuristics in strategic decision-making," Journal of business venturing 12:1, 9-30

Castelli, M., L. Manzoni, and A. Popovi , 2016, "An artificial intelligence system to predict quality of service in banking organizations," Computational Intelligence and Neuroscience 2016, article ID 9139380

CBC News, 2017, "TD Bank shares post worst day since 2009 after CBC story," March 11, http://bit.ly/2tFHcxV

CCP, 2015, "20 banks, five years and £252Bn in conduct costs," Conduct Costs Report 2015, CCP Research Foundation http://bit.ly/2tFIlFF

Chang, S. I., D. C. Yen, I. C. Chang, and D. Jan, 2014, "Internal control framework for a compliant ERP system," Information & Management 51:2, 187-205

Cocca, T. D., 2016, "Potential and limitations of virtual advice in wealth management," Journal of Financial Transformation 44, 45-57

Evans, L. T., and N. C. Quigley, 1995, "Shareholder liability regimes, principal-agent relationships, and banking industry performance," Journal of Law and Economics 38:2, 497-520

Gallagher, B. P., P. J. Case, R. C. Creel, S. Kushner, and R. C. Williams, 2005, "A taxonomy of operational risks," Software Engineering Institute, Carnegie Mellon University, http://bit.ly/2vWj06K

Grody, A. D., and P. J. Hughes, 2016, "Risk accounting-part 1: the risk data aggregation and risk reporting (BCBS 239) foundation of enterprise risk management (ERM) and risk governance," Journal of Risk Management in Financial Institutions 9:2, 130-146

ISO/IEC Guide 73:2002, Risk management – vocabulary – guidelines for use in standards, http://bit.ly/2uVi99s

Jarrow, R. A., 2008, "Operational risk," Journal of Banking & Finance 32:5, 870-879

Jessel, B., and T. Marshall, 2016, "Get bold with blockchain," Journal of Financial Transformation 43, 15-20

Kahneman, D., 2003, "Maps of bounded rationality: psychology for behavioral economics," American economic review 93:5, 1449-1475

Kaplan, R. S., and D. P. Norton, 1996, The balanced scorecard: translating strategy into action, Harvard Business Press

Kegan, R., and L. L. Lahey, 2001, "The real reason people won't change," Harvard Business Review 79:10, 84–92

Kim, S. D., 2014, "Characterization of unknown unknowns using separation principles in case study on Deepwater Horizon oil spill," Journal of Risk Research 20:1, 1-18

Liao, H. H., T. K. Chen, and C. W. Lu, 2009, "Bank credit risk and structural credit models: agency and information asymmetry perspectives," Journal of Banking & Finance 33:8, 1520-1530

Luft, J., and H. Ingham, 1961, "The Johari Window: a graphic model of awareness in interpersonal relations," Human Relations Training News 5:9, 6-7

McCreary, D. and A. Kelly, 2013, Making sense of NoSQL, Manning Publications

Mikes, A., 2008, "Chief risk officers at crunch time: compliance champions or business partners?" Journal of Risk Management in Financial Institutions 2:1, 7-25

Mikes, A., and R. S. Kaplan, 2015, "When one size doesn't fit all: evolving directions in the research and practice of enterprise risk management," Journal of Applied Corporate Finance 27:1, 37-40

Moosa, I., 2007, Operational risk management, Springer

Morris, J. J., 2011, "The impact of enterprise resource planning (ERP) systems on the effectiveness of internal controls over financial reporting," Journal of Information Systems 25:1, 129-157

Nelson, S. C., and P. J. Katzenstein, 2014, "Uncertainty, risk, and the financial crisis of 2008," International Organization 68:2, 361-392

Ormerod, P., 2007, Why most things fail: evolution, extinction and economics, John Wiley & Sons

Petraeus, D., 2015, Foreword: "Social science goes to war: the human terrain system in Iraq and Afghanistan," McFate, M., and J. H. Laurence (eds.), Oxford University Press

Rockart, J. F., 1979, "Chief executives define their own data needs," Harvard Business Review 57, March-April, 81-83

Rosemann, M., and M. Zur Muehlen, 2005, "Integrating risks in business process models," ACIS (Australasian Conferences on Information Systems) 2005 Proceedings 50, http://bit.ly/2uT7gFx

Sadgrove, K., 2016, The complete guide to business risk management, Routledge

Shojai, S., and G. Feiger, 2010, "Economists' hubris - the case of risk management," Journal of Financial Transformation 28, 25-35

Simon, H. A., 1955, "A behavioral model of rational choice," Quarterly Journal of Economics 69:1, 99-118

Soares, S., 2015, The Chief Data Officer handbook for data governance, MC Press LLC

Stanton, T. H., 2012, Why some firms thrive while others fail: governance and management lessons from the crisis, Oxford University Press

Stulz, R. M., 2015, "Risk-taking and risk management by banks," Journal of Applied Corporate Finance 27:1, 8-18

Taleb, N. N., 2005, The black swan: why don't we learn that we don't learn, Random House

Taleb, N. N., 2012, Antifragile: things that gain from disorder, volume 3, Random House

Tett, G., 2010, "Silos and silences. Why so few people spotted the problems in complex credit and what that implies for the future," Financial stability review 14, 121-129

WEF, 2016, "The role of financial services in society: understanding the impact of technology-enabled innovation on financial stability," World Economic Forum, http://bit.ly/1qCGJWN

Zuboff, S., 1991, Informate the enterprise: an agenda for the twenty-first century," National Forum 71:3, 3-7

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward. Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, and finance, risk & compliance. We also have an energy consulting practice. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Xing.**

WORLDWIDE OFFICES

Bangalore
Bratislava
Brussels
Chicago
Dallas
Dusseldorf
Edinburgh
Frankfurt
Geneva
Hong Kong
Houston
Kuala Lumpur
London
New York
Orlando
Paris
Pune
São Paulo
Singapore
Stockholm
Toronto
Vienna
Warsaw
Washington, DC
Zurich

CAPCO.COM

CAPCO