2019 Enterprise Risk Management Symposium

May 2–3, 2019, Orlando, FL

Enterprise Risk Management (ERM): Key Risks, Responses and Applications

Garfield Francis

Enterprise Risk Management (ERM): Key Risks, Responses and Applications

Garfield Francis

Abstract

As a member of the Society of Actuaries (SOA), I've taken on numerous roles over the course of my career. I started as an analyst, working primarily on data management. This highly technical role involved a lot of data manipulation and process automation within Excel and Access. I later moved into the role of assistant actuary, where I drove the conversion and redesign of the retirement plan predictive models by providing data and reporting analytics support, communicating across functional teams and conducting source-of-earnings and attribution analysis. Additionally, I utilized these stochastic and deterministic financial projection models to actively contribute to the analysis (involving the identification and measurement of key risk drivers); communication of results; design and planning of long-term liability projections such as embedded value, economic capital, asset adequacy testing and budget valuation. In my most recent role, on the pension risk transfer research and development team, I assisted in the pricing of U.S. funded buyout pension deals as well as the development of the U.K. longevity reinsurance collateral models.

I'm currently a chair for the SOA's Project Oversight Group. In this role, I use my knowledge and experience of financial and risk management methods and tools to help provide research that contributes to the intellectual capital of the actuarial profession and advances our knowledge base. I'm also a member of the Predictive Analytics Council. Although I'm relatively new to the council, this topic has been a passion of mine since the start of my actuarial career. I find the use of past data to make inferences about the future to help companies manage their risk and uncertainty to be highly fascinating. In addition to this, I'm a member of the Investment Section.

The purpose of this paper is to discuss various types of risks within an enterprise risk management (ERM) framework, responses to those risks and the implementation of an ERM framework. The key risks to be discussed include financial risk, market risk, physical assets risk, operational risk, strategic risk, reputational risk and supply chain risk. Although ERM is a relatively new term, the concepts that encompass an ERM framework have been in practice for generations. It is only recently that these concepts have been thoroughly examined and properly subdivided into the seven risk classes identified here. In addition to a discussion of these risk types, this paper aims to identify how to properly respond to such risks by either reducing, removing, transferring or accepting the risk.

Considering the scope of this paper and the broad range of risks being discussed, the idea being debated can be considered both theoretical as well as applied. The goal of this paper will therefore be to discuss the risks individually to better understand each, identify areas in which

they overlap, demonstrate ways to respond to them and show the methods by which they fit into an ERM framework. Additionally, the paper will delve into some of the current types and applications of the ERM platform. These applications include discussions on current processes that are being used in the measurement and management of risk and how these processes take shape within an organization.

To write this paper, I referred to the work of one of the most noted authors on this subject, Paul Sweeting (2017), as well as my own experience working in risk management. I chose this topic, in part, due to my belief in how important the ideas of this framework are in contributing to the overall stability of the management of companies and the overall health of the economy. Having worked through the 2008 global financial crisis and witnessed the hardship that resulted from inappropriate managing of risk illustrates why this paper and its findings are important. The problems in the U.S. housing market spread to the real estate market in Europe and to the banks with exposures to that market. The federal government bailed out the banks, cut spending and borrowed heavily. It is my hope that the knowledge gained in writing and sharing this paper will lead to more fun and less hardship among all organizational levels and industries.

1. Introduction

One feature is typically common within any ERM framework. Most begin with first assessing the context of the operation. This involves understanding the risk management environment of the organization, which in turn requires an understanding of the organization's nature and its shareholders. In the process of making this assessment, drivers of the company's operations are determined and the key risk identified. It is important when completing this report to consider ways in which these risks are correlated. Correlation is an important concept in ERM, as a core part of the process involves aggregating risks. If two risks have a strong positive correlation, then the risk of both occurring simultaneously is high; if the correlation is low, then the risks can diversify one another; and if the correlation is strongly negative, then there is an incentive to increase the level of one risk in order to offset the second.

Once the context has been defined, the ERM process can be implemented as a control cycle. But it is important to note that this process is continual rather than one with a defined beginning and end. However, this is not to say that the context cannot change. Both internal and external factors will develop over time, so it is important to be constantly aware of the context and its impact on the process you are analyzing.

Regulations will differ depending on the type of institution being discussed as well as its country of domicile. While not specific, these regulations are separated into mandatory, advisory, and proprietary ERM frameworks. Often, the requirements needed to attain a certain level of confidence from a regulatory body will be stated explicitly, as will the process by which these standards were established. We will discuss additional guidelines within an insurance context, specifically from the actuarial standpoint.

2. Discussion of Risk Types

The first stage in a risk management process is identification of risk, but you must ensure that this is done using a consistent risk language and taxonomy. This involves not only defining all the risks, but also grouping them in a coherent fashion. This ensures that risks have consistent meanings throughout the organization. The major risks to consider during this stage are market risk, financial risk, physical assets risk, operational risk, strategic risk, reputational risk, and supply chain risk.

2.1 Market and Financial Risk

Market risk is the risk inherent from exposure to capital markets. It relates directly to the financial instruments held on the asset side (equities, bonds, etc.) and the effects of changes to the valuation of liabilities (e.g., long-term interest rates and their effect on life insurance and pensions liabilities). The most fundamental aspect of managing market risk is to have clear policies on the overall level of market risk that is acceptable by a measure such as value-at-risk (VaR), which is the maximum amount that will be lost over a certain holding period with a particular degree of confidence.

A close relative of market risk is financial risk (commonly referred to as economic risk). This risk covers price and salary inflation. While these risks affect different aspects of an organization—market risk affects the assets and financial risk the liabilities—there often will be overlap, where both can be modeled and accounted for in a similar way.

In both life and non-life insurance organizations, market risk is arguably the most significant risk faced. For non-life insurance companies, market risk is evident in the investments of marketable assets as well as the assumptions used for claims inflation. The extent to which this is true depends on the class of insurance; for example, case inflation can be driven by idiosyncratic factors such as medical expense growth. For life insurance companies and pension schemes, the market risk in the asset portfolio is linked to the various financial assumptions used to value the liabilities, or more precisely, the rate at which those liabilities are discounted.

Interest rate risk, a special category of market risk, arises from unanticipated changes in interest rates of various terms. Whether it is changes in the overall interest rates or in the shape of the yield curve, which is interest rates at different terms by different amounts. It affects the value of long-term financial liabilities and the value of fixed-interest investments. The term structure of interest rates is an important aspect of interest rate risk. Holding assets to hedge interest-sensitive liabilities is only effective if both are affected by various changes in interest rates in a similar way.

Foreign exchange risk is another special type of market or financial risk. It reflects the risk present when cash flows received are in a currency different from the cash flow due. This is a component of equity market risk when comparing domestic and overseas equities. However, the underlying cash flows of many domestic equities are from unhedged overseas sources, and in many cases a stock listed on an exchange in one country will have a similar pattern underlying cash flows to one listed elsewhere.

Liquidity risk is a financial risk faced by all institutions. This is the risk that a firm cannot meet expected and unexpected current and future cash flow and collateral needs. Life insurance firms generally have long-term liabilities and greater cash flow predictability than banks, so a higher degree of illiquidity is appropriate. Non-life insurance liabilities fall somewhere between bank and life insurance liabilities in terms of both term and predictability, depending on the class of business, so the appropriate level of liability is similarly variable. Pension schemes are generally long-term institutions; however, a pension scheme that is cash flow positive (where benefits are still being accrued at a higher rate than they are being paid out) can afford to invest a higher proportion of its assets in illiquid investments than can a cash flow negative scheme (a closed or even just a very mature scheme).

2.2 Credit Risk

In some cases, credit risk only refers to default risk. In other instances, it is limited to the risk of loss from nonpayment. Under this definition, the other main aspect of credit risk—that is, spread risk or the risk of a change in value due to a change in the spread—is covered by market risk. Additionally, there is an element of default risk inherent in traded securities. This too is typically

covered by market risk. But in relation to a particular security, it may include the risk of downgrade and, more generally, spread widening. This distinction is important because spreads can widen for a bond without that bond being downgraded. Credit risk, in the form of loans to individuals and small businesses, is often the most vital risk faced by banks, but another major source of credit risk is counterparty risk for derivative trades.

2.3 Physical Assets Risk

Physical assets risk is the risk that an organization will suffer financial losses due to some form of physical damage to its property. Some examples are major events affecting a whole city or country, such as an earthquake or hurricane. It might also be an event affecting only the firm, such as terrorism or vandalism. This risk is distinct from the losses suffered by an insurance company due to events affecting policyholders. It refers to damage to the organization's own assets and is distinct from any consequential loss. If an organization loses its office, it will lose money due to the need to replace the building and because it will not be able to carry out business in the meantime. Physical asset risk refers only to the first of these two losses.

When incorporating this risk into ERM, where operations are new and market information is evolving, it is pivotal that you think about the ways in which suppliers and business partners will be affected and the concentration of risk arising across suppliers or between your own organization and a supplier.

2.4 Operational Risk

Operational failures have led to the ultimate demise of more than one firm. This is because poor control of operational risk allows other types, such as market or credit risk, to become excessive. The most widely accepted definition of operational risk is the definition used by the Basel Committee on Banking Supervision (2011). This entity defines operational risk as the risk of loss resulting from inadequate or failed processes, people and systems or from external events. The definition covers risks that can result in direct financial losses to an institution. Operational risk consists of several different risks that tend to overlap to a significant degree. These may be crime, technology, cyber, regulatory, people, legal, model, data, reputation, project and strategic risks. Since measuring and matching operational risk exposures to loss experience can be difficult, firms tend to focus on controlling operational losses rather than quantifying them.

Given the many risks that comprise operational risk, it can be a difficult task to aggregate it across various business units within an enterprise. Instead of looking at the enterprise from the lowest level, it is most common to have an enterprise value that is then used to determine your operational risk. Here is a brief discussion of each of the risks included in operational risk.

Crime Risk

Losses due to crime risks may be defined as those resulting from the dishonest behavior of individuals in relation to a firm.

Technology Risk

This includes unintended loss or disclosure of confidential information, data corruption and computer system failure. This risk is very significant in an Internet-dependent world. System failure is particularly important if a company transacts a significant proportion of its business electronically or if many employees work remotely.

Clearly there is an overlap between technology risk and crime risk if the technological failure is deliberate, but another dimension of technology risk is that there are undiscovered errors in software used in an organization. Such errors might result in losses from mispricing or incorrect payments being made. The result could be a direct financial loss together with a loss of business resulting from a lack of client/consumer confidence.

Technology risk increases exponentially depending on the number of systems an organization has. This is most evident when firms using different systems merge.

Cyber Risk

This risk involves the failure of information technology systems, typically where there is online activity and the storage of personal data. A common type of internal cyber risk is data theft, by which client lists and contact details can be stolen or internal models copied. This can also

include employees' unauthorized access to data, such as colleagues' personnel files, and the risk that disgruntled employees can sabotage computer systems or maliciously change data.

A higher profile form of cyber risk is that which arises from external sources like hacking—gaining unauthorized access to internal systems. Again, this can result in the theft of data that is either commercially sensitive or sensitive to a firm's clients. Other issues include denial-of-service (DoS) attacks, where a firm's computer links, typically to the Internet, are disrupted in order to make its systems unavailable to users.

In addition to deliberate collusion between insiders and outsiders, there is a risk that employees may unwittingly facilitate cybercrime. For example, if an employee opens an email attachment that contains a virus, malware may be installed on that employee's computer and spread throughout the organization.

Regulatory Risk

This is the risk that an organization will be negatively impacted by a change in legislation or regulation or will fall foul of legislation or regulations that are already in place. To fully understand and account for regulatory risk, we must also consider employment, client and execution risks. A failure to comply with existing rules may bring fines or even expensive litigation.

As far as Basel classifications are concerned, these negative regulatory events cover employee relations, workplace safety and issues relating to diversity and discrimination. The Basel definitions cover only the direct costs. For a financial institution, this could well relate to compensation payments and losses linked to the termination of employment. However, losses resulting from organized labor activity—for example, strike action—are also covered. For most financial organizations, this might not seem like a major risk; however, there is a significant potential for issues such as repetitive strain injury from computer keyboard use, or eye and neck problems from the use of computer monitors, which can result in employee absences and loss of work time.

Falling short in the way it deals with its clients, sells its products and carries out business in general can result in significant losses for a firm. These losses can arise from a failure to meet a professional obligation to specific clients or from the inappropriate nature or design of a product. A key obligation in this regard is to ensure that products are suitable for the clients to whom they are sold.

In relation to clients, regulatory risk can include everything from the process of "onboarding" a new client through providing account information to that client, ensuring that the client's instructions are carried out promptly and correctly, and making sure that all client details are kept up-to-date. It also, of course, includes receiving premiums and contributions, and making payments. Within a firm, it relates to executing, recording and accounting for trades.

People Risk

This category can be reserved for noncriminal actions that may adversely affect an enterprise. Within the scope of this risk are indirect employment-related risks, adverse selection risks, moral hazard risks, agency risks and bias.

Indirect employment-related risks start with the risk that the wrong people are employed. It is important that employees have the skills an organization needs to run its business. This risk type can also include the risk of disruption caused by employees. As well as absence through industrial action, it can be as a result of sickness—possibly due to stress. While the negative publicity and widespread disruption caused by the former make it an important issue, the long-term damage to an institution caused by persistently absent employees can also be significant; in addition to the direct financial cost involved, morale can suffer.

Once employees have been recruited, it is important that the right ones are promoted and that such promotions are good for the organization. It is also important to retain the right employees. Losing employees can result in a loss of valuable intellectual capital and can damage the morale of remaining employees. It can also be expensive. Recruitment costs time and money, and every time a recruit is taken on, there is the risk that the employee is not right for the role or the organization.

Employment-related risks also include various aspects relating to contracts, dismissal, diversity, discrimination, and health and safety. As such, it can be said to incorporate the legal aspects of employment.

Adverse selection, particularly, arises from issues relating to underwriting risk in both life and non-life insurance. This is the risk that the demand for insurance is positively correlated with the risk of loss. Adverse selection arises as a result of asymmetry of information and the inability to differentiate between different risks when pricing. In extreme cases, it can lead to market failure, as with “Akerlof’s lemons” (Akerlof 1970). It is also an issue for banks, because individuals with poor credit ratings will be more likely to apply for loans with banks that do not charge higher rates to reflect the higher risks. It can even be an issue for defined-benefit pension schemes—if a pension can be commuted to a tax-free cash lump sum at an actuarially calculated rate, those having shorter expectations of life are more likely to commute their pensions.

If adverse selection involves failing to disclose information that could alter the terms of an agreement—for example, the level of insurance cover or the price of that cover—then it could be classified as fraud.

Moral hazard is the risk that clients’ behavior will depend on the level of their exposure to a particular risk. As with adverse selection, moral hazard is linked to the asymmetry of information, but it is more about the inability of an insurer to control the behavior of the insured once the insurance is in place. For example, if someone is more likely to juggle a set of lead crystal glasses because he or she has household contents insurance in place, then this is moral

hazard; if someone who enjoys juggling lead crystal glasses is more likely to buy household contents insurance, then this is adverse selection.

If the moral hazard results in potentially criminal behavior—for example, taking out insurance such that the lead crystal glasses can be smashed and the insurance payout claimed—then this counts as fraud.

Agency risk is the risk that one party appointed to act on behalf of another will instead act on its own behalf. Within insurance companies, the fact that the actuaries responsible for regulatory reporting are remunerated by the firms, which might be more focused on shareholder value than policyholder security, gives an example of agency risk. The costs arising from agency risks are agency costs. There are two main sources for these costs. The first is the loss associated with the action of the agents, and the second is the cost of any action taken to modify the behavior of agents.

Bias is a systemic risk that can be deliberate or subconscious. Deliberate bias arises if key risks are intentionally omitted or downplayed, or their consequence is misrepresented. Similarly, the link between different risks or the impact of the business or underwriting cycles might be understated. Biases can arise unintentionally. Risks can accidentally be forgotten or underestimated due to lack of data. However, it is difficult to determine the extent to which many of these accidents are true oversights.

Anchoring is another behavioral bias with clear implications in the world of finance. This occurs when decisions are made relative to an existing position rather than based solely on the relevant facts. The question asked is “Given where we are, where should we be?”; it should be “Given the relevant facts, where should we be?”

Representativeness (assuming that things with similar properties are alike) and heuristic simplification (using rules-of-thumb) can also be sources of problems in all financial organizations where the eventual level of risk may turn out to be very different to an initial estimation or approximation.

Legal Risk

This term describes the risk arising from poorly drafted legal documents within an organization. It extends to policy documents that form legal agreements between firms and policyholders. It can be linked to regulatory risk, since ambiguities in legal contracts may ultimately be dealt with by courts. Legal risk also includes exposure to fines, penalties or punitive damages resulting from supervisory actions and private settlements. Therefore, it cuts across a range of risks, including employment and client risks.

Model Risk

This is the risk that the financial models used to assess risk, determine trades or otherwise help make financial decisions are flawed. The flaws can be in the structure of a model, which may be

overly simplistic or otherwise unrealistic, or it can be in the choice of parameters used for an otherwise sound model. Model risk may also relate to the incorrect translation of model from theory into code, although this can also be thought of as an aspect of technology risk since it assumes that the model itself is sound.

Model risk can be mitigated by making sure there is a rigorous documented process for model coding together with a clear audit trail. It is also important to ensure that all models are designed for the situations in which they are used or that there is a sound reason for putting a model to another use. For example, a model may give reasonable estimates of the expected returns from a strategy and the range of results that can be expected in normal market conditions, but it might be very poor at predicting the range of adverse outcomes that may occur in stressed markets.

Data Risk

This type of risk cuts across execution, delivery and process risk, as well as client risk. It is the risk that incorrect data will be fed into a decision-making process (relating it to execution risk). Even if there is no deliberate misreporting, data may be entered incorrectly or fill-in codes may be used when information is not available.

A separate issue arises during data analysis when a single individual has several records in his or her name. This can skew any analysis carried out if duplicates are not removed or consolidated.

Reputational Risk

The risk that arises from other operational risks is known as reputational risk. For example, a loss of data—potentially a technology risk—can result in a loss of client confidence due to reputational damage. Similarly, repeated delays in claim payments by an insurance company is likely to be a process risk, but the subsequent loss of business due to a loss of confidence in the firm's brand is a reputational issue.

Project Risk

Project risk is an umbrella term covering all the various operational risks in the context of a project. In the case of financial institutions, such projects may include the creation of physical assets, such as property development for investment purposes or a new head-office building or the purchase of a new computer system for the institution.

Strategic Risk

This is like project risk in that it includes many of the operational risks covered previously. However, it involves a more fundamental subject—achievement of the organization's core objectives. The most basic strategic risk is that no coherent strategy for future development exists. If this risk is to be overcome, an organization must make a conscious decision about what its strategy is and how it intends to implement that strategy.

A key strategic decision that a firm needs to make is whether it will attempt to compete on price or through having a differentiated product. This decision allows for the quantification of this risk, which is often difficult to quantify since it interacts so thoroughly with other risks.

2.5 Supply Chain Risk

Supply chain risk is the implementation of strategies to manage both everyday and exceptional risks along the supply chain based on continuous risk assessment with the objective of reducing vulnerability and ensuring continuity. To identify key risk indicators of supply chain risk, you must consider the likelihood of an event's occurrence and its impact. The drawback of using this method to compute supply chain risk is that it requires assessing the likelihood or probability of many different event types for any number of supply chain locations (which can number in the hundreds of thousands).

To manage supply chain risks, you will need to attempt to reduce supply chain vulnerability via a coordinated holistic approach, involving all supply chain stakeholders, that identifies and analyzes the risk of failure points within the supply chain. Risks to supply chain range from unpredictable natural threats to counterfeit products and reach across quality and security to resiliency and product integrity.

3. Risk Responses

After you've had a healthy discussion on the various types of risk types your organization may face and considered its risk appetite, you next need to think about how you will respond to these risks. When considering this, you can place your response in one of four categories: reduce, remove, transfer or accept. This ensures that all potential responses are considered in relation to a risk as it arises.

Risk reduction involves taking active steps to limit the impact of a risk occurring. A common approach in this response category is diversification. This involves combining a risk with other uncorrelated risks, or at least with one or more risks whose correlation with the original risk is less than one. In the extreme, this becomes hedging when taking on risks that have a high negative correlation with the original risk faced. The reduction of risk can also involve the creation of more robust systems and processes. This allows for reducing the chance of a risk emerging or limiting the impact of a risk if it does emerge.

Another form of risk response involves the removal of the risk. This means making sure that the institution is no longer exposed to that risk at all. You can achieve this by choosing to avoid a project or an investment altogether or deciding to achieve its aims differently.

The most frequent response to risk is risk transfer. This involves shifting the consequences of a risk event to a different party. Two important categories exist under this type of response: noncapital market and capital market risk transfer. The transfer of noncapital market risk in its

most common form is insurance—the payment of a premium to buy protection from a risk. A traditional route is for a firm wishing to transfer a risk to pay a premium to another firm—the insurer—in exchange for protection. However, some firms choose to self-insure, either by setting aside assets or by setting up a wholly owned captive insurance company. Formal and informal captives can also be set up by groups of firms to achieve an element of diversification between them. Alternatively, capital market risk transfer—also known as securitization—is a way of turning risk exposure into an investment that can be bought and sold; here investors take exposure to the risk but earn a risk premium for doing so. One of the most common formats is to package risks in a bond where the payments to investors are reduced if losses rise above a certain level. An attractive feature of capital market risk transfer is that if the security bearing the risk is traded, then its price can be used to provide a market-based price for the risk. This means a market price can be determined for any risks of a similar nature to those transferred but are retained by the firm. Such marking to market is an important part of risk frameworks such as Basel II and Solvency II.

Accepting, retaining or taking a risk rather than reducing, removing or transferring it implies that no action is taken to respond to the risk. This can be done because the risk is trivial—either because the potential severity of the risk is small or because the probability of occurrence is highly unlikely—but large risks can also be retained. An additional aspect of retaining a risk is when that risk is part of the business plan. An example of this would be mortality risk taken by a life insurer.

A good risk response should have several features. It should be economical, meaning that the solution chosen should not only be the least costly way of achieving the results but also cost less than the amount saved in the reduction of risk. This can be both easy and difficult to quantify. For example, if a new expense monitoring system is introduced to reduce the number of fraudulent expense claims, then the cost of the system can easily be compared with the reduction in the total volume of expenses. However, if a strategy is put in place to reduce the chances of reputational damage, then it is much more difficult to assess whether that strategy has been cost-effective. It is also important to ensure that risk responses match the risks they are intended to control as closely as possible. However, this can involve a compromise with the principles of economy. For example, if you are trying to limit the downside risk of investments in a portfolio of mid-cap shares, options on that portfolio of shares might be thinly traded and therefore expensive. Linked to this point, responses should be as simple as possible to avoid mistakes. They should work both theoretically and practically, and they should be actionable (enforceable). Firms should also consider retaining risk unless the risk is significant.

4. Enterprise Risk Management Framework

The ERM framework looks at financial institutions, or even systems, and tries to manage all these risks in a consistent manner. Three Actuarial Standards of Practice (ASOPs)[1] are most applicable to insurance companies beginning to develop their ERM frameworks, as well as those who are in the process of updating a framework based on new regulations and increasing their capability and capacity. The standards are ASOP 7, "Performing Cash Flow Testing for Insurers"; ASOP 12, "Concerning Risk Classification"; and ASOP 23, "Data Quality." As part of the development process, and in addition to abiding by the stated ASOPs, insurance companies and other financial institutions need to identify the category of risk framework they will be implementing. Typically, an ERM framework will fall into one of three categories; mandatory, advisory or proprietary.

4.1 Actuarial Standards of Practice

ASOP 7, "Performing Cash Flow Testing for Insurers," applies to actuaries when performing the analysis of part or all of an insurer's asset, policy or other liability cash flows. The analysis subject to this standard should be considered in connection with professional services such as determination of reserves adequacy, determination of capital adequacy, product development or ratemaking studies, evaluations of investment strategy, financial projections or forecasts, actuarial appraisals, and testing of future charges or benefits that vary at the discretion of the insurer (for example, policyholder dividend scales and other nonguaranteed elements of the insurer's liabilities). This standard does not apply to actuaries when performing cash flow analysis for entities other than life, health or property/casualty insurers such as pension plans, retiree group benefit plans or social insurance programs.

ASOP 12, "Concerning Risk Classification," provides guidance to actuaries performing professional services with respect to designing, reviewing or changing risk classification systems used in connection with financial or personal security systems. Such professional services may include expert testimony; regulatory activities; legislative activities; or statements concerning public policy to the extent that these activities involve designing, reviewing or changing a risk classification system used in connection with a specific financial or personal security system.

Finally, ASOP 23, "Data Quality," guides actuaries in selecting data, performing a review of data, using data or relying on data supplied by others in performing actuarial services. This standard also applies to actuaries who are selecting data, preparing data, or are responsible for the selection or preparation of data that the actuary believes will be used by other actuaries in performing actuarial services or when making appropriate disclosures with regard to data quality.

[1] The current ASOPs can be found online at http://www.actuarialstandardsboard.org/standards-of-practice.

4.2 Mandatory Risk Framework

An organization must follow a mandatory risk framework to carry out some types of business. Basel II and Solvency II are the most important. Basel II is geared toward the banking sector, while Solvency II deals with insurance.

The Basel Accords constitute the global risk framework designed to promote stability in the banking sector. They are published and updated by the Basel Committee on Banking Supervision (BCBS). These recommendations are taken up not just by regulators in G10 countries, but also by those in other countries, where implementation differs. The first Basel Accord (Basel I) originally focused exclusively on credit risk, which can be thought of here as the risk that funds owed are not paid. The methodology behind Basel I was straightforward. First, credit-related assets and liabilities that were off-balance sheet were converted to on-balance sheet equivalents. These were then risk weighted, together with the existing on-balance sheet credit exposures. Very low risk assets such as AAA-rated government bonds had a risk weight of zero, while assets that were riskier—for example, unsecured loans—could have a risk weight of up to 100% of their face value. These risk-weighted assets were then summed, the total representing the level of risk to which the institution was exposed and multiplied by a minimum capital requirement of 8%. This meant that firms held an additional 8% of risk-weighted assets.

Later it became clear that banks were exposed to significant market risks, leading to an amendment to Basel I. Market risk here refers to the risk that the value of assets will move in such a way as to cause a financial loss. Under this amendment, exposures to market risk were calculated using either a risk-weighted approach (as for credit risk) or based on the firm's agreed internal model, which was usually calculated based on a 99% 10-day VaR. As previously stated, VaR is the maximum amount that will be lost over a certain holding period with a certain degree of confidence. However, a major problem still existed; the range of risk covered was still narrow. This resulted in many banks running into difficulties while appearing healthy under a Basel I framework. Operational risk, which was not covered under Basel I, often featured heavily in these cases.

The introduction of Basel II sought to address many of the issues with Basel I, both in scope and in process. Both frameworks reduce the risk measure to a single number. This is helpful as it allows many firms to be compared on a consistent basis. However, given the range of firms described and the risks aggregated, it is dangerous to place too much emphasis on a single measure of risk such as this. In fact, this figure is even less informative for Basel II since it incorporates a broader range compared to Basel I. Another drawback of Basel II is that the list of risks addressed remains incomplete; specifically, liquidity risk is given only cursory treatment. But a major improvement over Basel I was the allowance for operational risk, with the outcome from Basel II leading to the following three pillars:

- **Minimum capital requirements.** Like Basel I, Basel II uses tier 1, 2 and 3 capital with only minor changes. Similarly, it allows for market and credit risk, with market risk remaining unchanged. As with Basel I, market risk is calculated using either the risk-weighting approach or an internal model. But in terms of valuation, liquid assets outside the banking

book are marked to market (so the market value of assets is used), whereas illiquid assets are marked to model, meaning that the values are benchmarked, extrapolated or otherwise calculated from a market input.

Credit risk changed under Basel II. First, it allows for a greater range of creditors that looked to treat the different credits more equitably. Basel II also allows for something like the internal model used for market risk, in this case known as the internal ratings based (IRB) approach. With this change, market and credit risks can be treated consistently.

The greatest change from the first to the second Basel Accord is that an allowance is made for operational risk. Under Basel II, operational risk is defined as 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel Committee on Banking Supervision 2011).

- **Supervisory review process.** Basel II recognizes explicitly that holding capital is not a substitute for inadequate risk management, although the results of the review might be a requirement to hold additional capital against risks not covered under the minimum capital requirement.

  The regulator must pay attention to several aspects of the process. Interest rate risk should be considered, as should various aspects of credit risk, including concentration and counterparty risk. Regulators should also verify that the approach used to quantify operational risk is consistent with the business and that market risk is correctly measured.

- **Market discipline.** Basel II promotes transparency by requiring firms to publish details of their risks, their capital and the ways in which they manage risk. It aims to ensure that enough information about the firm is disclosed for the market to assess the risks faced by the firm and for the cost of capital—the price of equity and debt—to be adjusted accordingly.

The fallout from the global financial crisis, in addition to the deficiency mentioned earlier, has led to parts of the first pillar of Basel II being strengthened under what is being called Basel III. This improved framework also introduces new liquidity requirements. Although implementation has begun, full compliance is not required until 2019.

Solvency II, an update of Solvency I, is the risk framework for insurance companies operating in the EU member states. It is modeled on Basel II but sponsored by the EU rather than G10 countries. Unlike the BCBS, the EU can require member states' adherence to its directive. Like Basel I, Solvency I made a strong attempt to provide a consistent and robust basis for solvency among insurers but fell short on many of the same issues: it was inflexible, different assets were treated as though they were identical, and it concentrated on too few risks. Solvency II is an attempt to address these issues. It is built around the following three pillars:

- **Quantitative requirements.** The two parts of this pillar are the solvency capital requirement (SCR) and the minimum capital requirement (MCR). The SCR is the main standard by which solvency is measured, and the MCR is the lower capital requirement. Any firm falling below the MCR loses its authorization. The SCR must be achievable with a 99.5% level of

confidence over a one-year time horizon. In contrast, the MCR is an objective calculation of how the firm should be able to meet the MCR with a probability of 80% to 90% over a one-year period.

The components of the basic solvency capital are non-life underwriting risk, life underwriting risk, special health underwriting risk, market risk (including interest rate mismatch), counterparty risk, and operational risk. Under this basic standardized approach, required reserves are calculated according to a specified deterministic basis, although stochastic methodology is often required, particularly in the valuation of with-profits guarantees.

Instead of this standard approach, a quantitative model designed by the firm can be used, but to be accepted by regulators, it must fulfill six criteria. These criteria are the "use test," statistical quality standards, calibration standards, profit and loss attribution, the validation standards and documentation standards.

- **Qualitative requirements.** This pillar is more of a message to regulators about how to treat firms than it is a rule for firms about how they should behave. For example, regulators should analyze the strategies of firms, suggesting that business models are under scrutiny.
- **Disclosure.** This pillar aims to improve the risk management process by encouraging firms to control risk to reduce the cost of capital.

Solvency II and Basel II are both designed with multinational organizations in mind. Additionally, they both have a three-pillar risk management framework that ensures that more capital is allocated to firms that run higher risks and that capital is not the only answer to risk management. Although similar, there are major differences between the two frameworks, with Solvency II being less prescriptive than Basel II.

Unlike Basel III, Solvency II does not have any specific requirements in relation to liquidity. The capital raised by banks is traditionally short term, including current accounts. Insurance companies, on the other hand, have no equivalent source of financing, which is more likely to be funded by "traditional" forms of bond financing. The companies are also less likely to face immediate liquidity needs. Life insurance generally has predictable cash flows, while the settlement times for non-life insurance are generally months or years rather than days.

4.3 Advisory Risk Framework

An advisory risk framework is not required for legislative compliance but can be helpful when defining an ERM framework. The following are samples of advisory risk frameworks.

Risk Analysis and Management for Projects (RAMP)

This is the methodology for the management of risks in any kind of project. The stages within this process include RAMP launch, risk identification, risk analysis, financial evaluation, risk mitigation, go/no-go decision, risk control and RAMP closedown.

RAMP is intended for use with capital projects rather than in an ongoing business, a decision on whether to proceed at all is required, and post-project closedown analysis forms are part of the process. Risk is expressed in financial terms using an investment model that facilitates decisions on whether projects should go ahead or not and, if so, in what form.

COSO ERM Integrated Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) document details how ERM encompasses aligning risk appetite and strategy, enhancing risk response decisions, reducing operational surprises and losses, identifying and managing multiple and cross-enterprise risks, seizing opportunities and improving the deployment of capital.

This document describes the context and scope of risk management with a three-dimensional matrix. Each dimension is inextricably linked to the others. The first of these dimensions is the range of areas that the risk framework should cover. The framework divides these areas into operational, compliance, reporting and strategic categories. The second dimension described in the framework covers internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. Lastly, the third dimension of the framework is the level of application. This emphasizes that risk management applies to all levels of an organization, from the entity through divisions, business units and subsidiaries.

The COSO document places ultimate responsibility for the framework with the CEO but points out that everyone has some role in risk management. This is true for the board, senior management and staff, regulators, professional organizations and educators.

The framework also explicitly describes the limitations of ERM, noting that in a risk management framework, processes may be inadequate, and human error can occur. Also, the benefits and all components of ERM need to be considered against the cost of implementation.

IRM/Alarm/AIRMIC 2002 Risk Management Standard

Although Airmic has withdrawn its support of this framework in favor of the new global standard ISO 31000:2009, the framework is still useful—not least because it is free to download.

It has several similarities with the COSO framework. For example, it defines risk in terms of a combination of the probability of an event and its consequences. Additionally, it recognizes that risk can have both upsides and downsides but focuses firmly on downside risk.

Risks are classified as internally and externally driven, and they are divided into financial, strategic, operational and hazard risks.

Some recommendations under this framework include that the risk identification process should be approached methodically and that an in-house approach is likely to be more effective than an approach that uses external consultancies. The framework emphasizes that the reporting of risks is part of good corporate governance and refers to both internal and external reporting, with an

internal audit being an important control. An important distinction is made between internal reporting—for the benefit of the board of directors, business units and individuals within an organization—and external reporting for investors and regulators.

Under this document, the risk management function is seen as the primary champion for risk management in the organization. It is responsible for setting risk management policy and strategy, building a risk management culture, educating employees, establishing structures and policies within business units, designing processes, coordinating functions, developing responses to risks and reporting risk.

For estimation purposes, the framework points out that a quantitative, semiquantitative or qualitative approach can be used, and that both threats and opportunities should be considered.

Treasury Board of Canada Integrated Risk Management Framework

The most recent version of this framework was issued in 2010 and was designed to help government officials in manage risk. It aims to accomplish this by the following methods:

- Identifying and explaining different risk types
- Making decisions and providing guidance on levels of risk tolerance and the treatment of risks
- Supporting continuing professional development
- Embedding risk management principles and practices in organizations
- Aligning officials' approach to the risk management practices and policies of the Treasury Board of Canada
- Supporting wider government policies
- Managing risk in a way that recognizes external and internal risk management contexts
- Adding value through risk management
- Balancing responses to risk with innovation
- Being transparent, inclusive, integrated and systematic
- Improving the culture, capacity and capability of risk management in organizations

The 2010 version of this report was supplemented by a guide to integrated risk management (Treasury Board of Canada 2016), which elaborated on the principles in the framework and aimed to give practical guidance and considerations for putting these principles into practice.

Orange Book

This framework is designed to give general guidance on risk management in both the public and private sectors. Its purpose is to operate at a higher level than other risk management standards, so other standards can operate within the framework set out in the Orange Book.

Starting with risk identification, the framework makes a distinction between initial and continuous identification. Prioritization rather than quantification is the focus here, with classification into high-, medium- and low-risk categories being considered. Next, risk appetite is

discussed in terms of a series of boundaries, limiting the risk that can be taken in different departments. In terms of risk response, the four approaches are referred to as tolerate, treat, transfer and terminate. Risk treatments are classified as preventive, corrective, directive and detective.

Regular reviewing and reporting are recommended, with the ultimate responsibility for these activities resting with the audit committee.

AS/NZS 4360:2004

This 2004 version was the third revision of the Joint Australian/New Zealand Standard. It is a relatively high-level document that has fewer stages than some comparable frameworks, and it is the predecessor to many of the other frameworks that exist today. It was used as the first draft for the global risk management standard ISO 31000:2009, the local version of which has been adopted in Australia and New Zealand as the successor to AS/NZS 4360:2004.

The first stage in this process is to establish the context within which risk management will be carried out. The next stage is risk assessment, which encompasses identification, analysis and evaluation. After the assessment of risks, their treatment is discussed at a high level. Communication and consultation with stakeholders—both internal and external—should take place throughout the process. The standard also considers how the risk management process can be made more effective.

ISO 31000:2009

ISO 31000:2009 has three broad sections covering principles and guidelines, the risk management framework and the risk management process. It also includes sections on risk management techniques and the vocabulary of risk management.

This standard defines risk as the effect of uncertainty on objectives. This can be regarded as an important shift of emphasis from the possibility of an event to the possibility of an effect—specifically, an effect on an objective. Unlike other frameworks, ISO 31000:2009 holds organizations, as well as managers, accountable for risk management.

This process is very similar to that of AS/NZS 4360:2004. The most notable difference is that monitoring and review replaces residual risk reporting as a more integral part of the process.

4.4 Proprietary Risk Frameworks

Credit rating agencies are stakeholders in a risk management context. They provide information to an institution’s investors and bondholders. The qualitative methods used by many of these agencies to rate bond issuers can be considered risk management frameworks in themselves. The three rating agencies are Fitch, Moody’s, and Standard & Poor’s.

Fitch determines its ratings based on information gained from public sources and through private meetings with issuers. Analysts' research is assessed by a ratings committee, which gives a rating based on a consensus decision. The following factors are used to a greater or lesser extent to determine the appropriate rating for each firm.

- **Industry risk and operating environment.** An industry may be in decline or thriving, may have high levels of competition or significant barriers to entry, may be capital or labor intensive, or may be inherently risky or safe. These factors are then overlaid with differences in financial management and country risk profiles affecting each industry.
- **Company profile.** Covered under this factor is the company's ability to prosper in the face of competition through product innovation and diversity.
- **Management strategy and corporate governance.** The firm's corporate strategy, risk tolerance, funding policies and capital structure are analyzed when determining its credit rating. Also important is the firm's corporate governance, as it will impact the effectiveness with which strategies are implemented.
- **Ownership and group structure.** This factor covers the relationship between the issuer of a bond and its parent company.
- **Financial profile.** This area focuses on the firm's cash flow and considers its ability to raise further funds. The firm's cash flow is linked to its capital structure. Preferred stocks are treated as quasi-debt, while contingent liabilities and pensions also receive special attention. Account policies, specifically the methods used to construct the accounts, are also considered.

Moody's Investors Service's ratings cover almost all the U.S. bond market. The starting point is the macroeconomic picture, where political, economic and industry considerations are examined. The analysts then look at a company's operating and competitive position.

Standard & Poor's assigns an individual analyst to each firm. The rating technique tends to differ based on the analyst, but the principles are broadly the same. The Standard & Poor's rating framework is divided into business analysis and financial analysis. However, the credit rating for a corporate entity can also depend on the creditworthiness of the country in which the firm is based. This framework is composed of three risk categories: sovereign risk, business risk and financial risk.

Under sovereign risk, countries can demand cash flows before they are distributed to overseas creditors, often through the mechanism of taxation. They can also establish currency controls or impose other regulations that make it hard for firms to pay creditors. Governments also have a broader impact on the environment in which a firm must operate and, therefore, its profitability. The analysis of business risk starts with a rating of each company's environment, particularly in relation to the industry in which the firm operates, with the industry considerations concerning long-term prospects for growth, stability or decline, and cyclical factors. If the firm is operating in different industries, the rating process also allows for diversification benefits. Using audited data, the starting point in the analysis of financial risk is to analyze the firm's profitability by considering the range of financial ratios. At least as important to Standard & Poor's is the

attitude that management takes to financial policy. This comprises aspects such as leverage targets, which includes both long-term and short-term debt financing, liquidity management, capital structure and the degree of financial flexibility.

5. Conclusion

The process that encompasses an enterprise risk management framework is far-reaching. Once the key risks have been identified, it is crucial that they are then reviewed in the context that is appropriate for the appetite of the organization. In practice, the organization's risk appetite should be agreed and given in clear terms before risks are measured. To do this, it is pivotal that the risk measures to be used are specified and that the values of those measures are thought to be acceptable.

This process involves determining the way in which risks will be analyzed, meaning whether a qualitative or quantitative approach will be used. These and other factors are included in a risk register. There are four broad areas to risk identification. The first concerns the tools that can be used, while the second concerns the ways in which the tools are employed. The third area is an initial assessment of the nature of the risk, and the fourth is the way in which the risk is recorded.

Once risks have been analyzed, the results must be assessed. This is true whether considering a project to be initiated, a product to be launched or an asset allocation to be implemented. Such analysis will generally involve trying to maximize (or minimize) one variable subject to a maximum (or minimum) permissible level of another variable. Creating these variables often involve applying particular risk and return measures to items. To do this, companies have been building more advanced risk management tools that allow them to produce a more detailed assessment of their risks. These tools are built around the risks and frameworks that are discussed in this paper. The outcome of this has resulted in risk management projects such as Efficient Frontier, Economic Capital, and Regulatory Capital.

Efficient Frontier can be thought of as a method for assessing an investment portfolio. Formally it is the set of portfolios that satisfies the condition that no other portfolio exists with a higher expected return but with the same standard deviation. For calculating Economic Capital, you need to bring together many of the risk principles discussed in this paper, covering risk measures and aggregation details. Borrowing an analytical framework from the life insurance and annuity industry, Economic Capital is framed in terms of the total assets required to remain solvent over a one-year period with a high level of confidence (Ai et al. 2015). Regulatory Capital is another form of risk assessment tool. This form of capital approach is factor driven, where the factor for each risk category is prescribed by the regulating body.

Having not only identified and analyzed the risk, but also compared it to the stated risk appetite of the organization, the next stage is to respond to those risks. Responses are categorized as reduce, remove, transfer or accept. The main purpose of these groups is to ensure that all potential responses are considered in relation to a risk as it arises.

It’s important to note that within financial companies, you will find qualified professionals. Their qualification standards often require that additional guidelines be followed within an ERM framework. The standards for insurance companies and their actuaries are known as the Actuarial Standards of Practice. The standards that are relevant in this context are ASOP 7, covering cash flow testing for insurers; ASOP 12, dealing with risk classification; and ASOP 23, pertaining to data quality.

References

Ai, Jing, Patrick L. Brockett and Allen F. Jacobson. 2015. “A New Defined Benefit Pension Risk Measurement Methodology,” *Insurance: Mathematics and Economics* 63: 40–51.

Basel Committee on Banking Supervision. 2011. “Principles for the Sound Management of Operational Risk.” Basel, Switzerland: Bank for International Settlements. https://www.bis.org/publ/bcbs195.pdf.

Sweeting, Paul. 2017. *Financial Enterprise Risk Management*. 2nd ed. New York: Cambridge University Press.

Treasury Board of Canada. 2016. “Guide to Integrated Risk Management.” Government of Canada. https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/guide-integrated-risk-management.html.

Garfield Francis, ASA, is an executive at Prudential in Newark, New Jersey. He can be reached at *Leobancroft@hotmail.com*.