

Risk Engineering for Financial Institutions

With a range of risk exposures currently facing financial institutions, Ian McNeil and Kevin Parker, from Zurich Risk Engineering, discuss the predominant issues facing risk managers and senior decision makers.



Ian McNeil

Global Head of Customer Management
Risk Engineering
Zurich Insurance Company Ltd



Kevin Parker

Head of Customer Management (EMEA)
Risk Engineering
Zurich Insurance Company Ltd



Ian McNeil

Global Head of Customer Management, Risk Engineering, Zurich Insurance Company Ltd

T: +44 (0)77 1003 8416 E: ian.mcneil@uk.zurich.com

Risk & Compliance Magazine (R&C): *Could you provide an overview of the range of risk exposures currently facing financial institutions (FIs)? What are the predominant issues keeping risk managers and other senior decision makers awake at night?*

McNeil: We evaluate the risk exposures facing financial institutions (FIs) across five main categories: market risks, people risks, organisation risks, strategic financial risks and operational risks.

In terms of market risks, an area which is particularly highly regulated, there is a lot of competition, with new entrants arriving in the online space, leading to different ways of doing business. For example, it is now rare for people to physically visit a bank branch, so the whole model has changed over the past few years to become reliant on technology. However things can go wrong. For example, a few months ago, TSB's online banking app failed to work properly. The problem received widespread coverage in the press and the chief executive was placed in front of a parliamentary committee to account for the system's failure.

In terms of people risks, there are many highly qualified, highly skilled people working in financial services, and many are waiting to see what the full impact of Brexit will be and whether headquarters will be relocated outside of the UK. This could mean losing staff and a subsequent struggle to attract new recruits.

Strategically, reputational risk is a key issue. At the moment it seems that FIs are not popular with the general public or with parliament, for that matter. This is a cause for concern, especially given the regulatory scrutiny the financial sector is under.

"In terms of market risks, an area which is particularly highly regulated, there is a lot of competition, with new entrants arriving in the online space, leading to different ways of doing business."

Ian McNeil,
Zurich Insurance Company Ltd

In terms of financial risks, the key aspect is the general economic environment. Are people borrowing money? Are they defaulting on loans? Are they looking at alternative revenue streams? Is there potential liability surrounding the advice given by FIs? Another issue is fraud and collusion within the banking sector, and the knock-on effect for share prices.

Finally, in terms of operational risks, the main concern is protecting the physical assets of a company – its people and its facilities – and ensuring safety across the working environment.

From a risk engineering perspective, dealing with these five categories of risk is what insurance coverage, and the risk assessments which underpin them, is all about.

R&C: *In what ways can risk engineering assist FIs to improve their loss prevention and risk management strategies? What do you believe are the most important components of an effective risk engineering system?*

Parker: There needs to be a tangible link between the risk engineering services provided by insurers and the insurance products that FIs actually buy. Risk engineering should not be perceived as a service purely designed to provide an underwriter with the assurance it requires in order to correctly accept and price risk. Risk engineering is more than that. It is a service which sits alongside insurance coverage but is not necessarily subservient to it. It should provide trusted advice as part of a true consulting partnership. Rather than approach risk engineering purely from an operational risk point of view, it is important to take a 'top down' view of exposures and offer a complete insight into business resilience, to truly understand and mitigate the total cost of risk. This requires working collaboratively with FIs, and deploying various tools and processes, to embed a robust and consistent risk management methodology, including risk profiling and hazard analysis.

Ultimately, the framework should provide visibility in terms of risks faced, as well as create data transparency so that information can be freely shared with key stakeholders. Risk engineering is a 'top down' approach which embeds the right behaviours, philosophies and tools. Alongside that is ongoing training to educate FIs on key issues affecting their business, including data protection, systems protection, cyber threats, as well as risks outside the company, such as those posed by supply chains and vendors, for example.

R&C: *To what extent is it necessary for FIs to adopt a holistic approach to risk management? What exactly does this mean from a practical standpoint?*

McNeil: The financial services sector has a mature business model. FIs already tend to take holistic approach toward risk and risk management, covering all of the five key risk areas mentioned earlier. But FIs need a clear, overarching view of the interconnectivity of the key risks they face and the regulatory landscape they occupy. First of all, such a framework should identify and understand the various risks. In our experience, this means having discussions with people at ground level, those who are on the 'front lines' – it cannot be done from the top floor of an office building.

Once risks have been identified, they must be assessed. Are they likely to happen? What may be the frequency? What sort of impact could they have? To answer these questions, experts may be brought in, but in-house expertise should also be utilised. A framework will assist in ranking and collating those risks. It also provides structure, helps inform decisions and establishes the FI's risk tolerance level. Can we accept that risk or do we need to do something about it? Can we insure it? If we cannot insure, what do we need to do? If we can insure, how can we improve coverage? Once an FI reaches the point of knowing what it can do, it might decide to stop doing it or utilise other risk improvement mechanisms.

It is important, however, to take action. A common trap is for a company to establish a robust risk management programme but then do nothing with it. Everything needs to be followed up, with any risk improvement or mitigation strategy tracked, monitored and controlled.

R&C: *How important is it for FIs to embed a risk management culture across their organisation? How can they achieve this?*

McNeil: Risk management has achieved a higher profile in recent years. Fifteen years ago, a risk manager sat alongside the team that bought the insurance. I do not believe that is the case today. Now, risk managers are at board level, or part of the chief financial officer team. Typically, the chief executive, the board and the chairman drive the philosophy surrounding risk management. They are focused on the bigger risks that a company faces – market, financial and strategic – and with embedding risk management in to organisational culture. Risk needs to be taken into account whenever a company makes a decision. If it is moving to new premises, entering a new market or launching a new product, there needs to be a risk management stress test and the right questions must be asked.

Kevin Parker

Head of Customer Management (EMEA), Risk Engineering, Zurich Insurance Company Ltd

T: +44 (0)78019 755 68 E: kevin.parker@uk.zurich.com



“There needs to be a tangible link between the risk engineering services provided by insurers and the insurance products that FIs actually buy.”

Kevin Parker,
Zurich Risk Engineering

Risk must also be embedded in objectives. Responsibility should not just be left with a risk management team at head office; it needs to be filtered throughout a company so that everybody, to some extent, has a risk objective as part of their behaviour. This is one way of ensuring that risk is embedded across a company, with everyone having some responsibility and accountability for risk.

R&C: Given the uptick in regulatory scrutiny of FIs, how might a redesign of their business operating models assist them to manage risk and control costs?

Parker: All FIs face pressure to maintain regulatory compliance. With fines increasing and individuals being held personally responsible for certain breaches, it has never been more important from a regulatory standpoint for businesses' operating models to be as robust as possible. It is a question of building these models to reflect wider risk. When it comes to making key decisions, a robust process is needed – with checks and balances, embedded within project risk management.

Ideally, a key stage needs to be introduced into the decision-making process to audit against, such as a checklist which outlines the risks and whether they have been effectively addressed. A methodology developed in conjunction with a risk engineering provider should also be utilised. This methodology should be transparent, well-documented and, most importantly, ensure there is a robust follow-up. It is all well and good producing some kind of risk register and employing a line of tolerance in terms of what is acceptable and what needs to

be mitigated, minimised or avoided, but the follow-up allows for continuous dialogue in the decision-making process and should be treated as a key part of the process.

R&C: What advice would you offer to FIs on using risk engineering to avoid major financial and reputational damage, and to ensure a competitive and sustainable future?

Parker: FIs should engage with a risk engineering service provider and discuss business sustainability, business resilience and the total cost of risk. A starting point in that journey is some kind of diagnostic workshop, where there is a degree of skills and knowledge transfer. That allows a risk consultant to fully understand any potential gaps in the existing risk management approach. This is normally achieved via a scenario planning activity, using real-life examples, so the risk consultant can ascertain how a customer would respond in certain types of situations. The collaborative workshop process should consider potential cost situations, look at gaps, demonstrate business and risk management approaches to resolving the situation, and recommend potential solutions.

For many FIs, risk-based interventions only become apparent once a loss has been sustained. Risk engineering, done in advance, puts FIs on the front foot when it comes to these scenarios. Running scenarios and looking at ways to implementing improvements is the better approach, rather than being reactive. To do this requires FIs to understand where they are culturally, from top to bottom of the company. Leveraging hazard analysis and risk profiling methodology tools and expertise is essential.

R&C: How do you expect risk engineering to evolve in the years ahead? In an increasingly complex and competitive environment, how confident are you that FIs understand the risks they face and how to manage them?

McNeil: Risk engineering has certainly evolved over the years. On the people side, it is moving more toward consultancy. Previously it was more of a transactional relationship, where recommendations would be put to FIs on behalf of an underwriting team. Over the last five years or so, that has certainly changed. Now it is more of a win-win partnership approach. The process involves talking to FIs and finding out what their goals are from a risk management perspective, then working with them collectively to achieve those goals. The relationship is closer.

Looking to the future, it is going to be about people skills, as well as innovation and empowerment. A key area of progress is data management – being able to delve into data in industry segments and notify FIs of the things they really need to be thinking about. Honing this process and making it more bespoke leads to a powerful risk management combination. As well as the evolution of hazard analysis and risk profiling, the way in which risk insight is shared is also changing. There is a lot of discussion pertaining to the ethos of sharing risk data, such as white papers, anonymised loss information and remedial actions that could have been taken to mitigate loss in real life scenarios. Combining risk consulting with empowering tools, innovation and data transparency will help FIs to understand both existing and emerging risks, and how to manage them.

Financial Institutions

Risk Engineering for Financial Institutions

If you would like to discuss any of the issues raised in this white paper, please contact Ian McNeil or Kevin Parker using their details below:

Ian McNeil is a qualified senior risk management and insurance professional, with over 35 years' experience of UK and global markets gained with multinational insurance companies and insurance brokers. Mr McNeil has proven strategic planning, business development, customer relationship and project management skills. He has worked in most insurance and risk management disciplines and performs effectively at all organisational levels, with the ability to manage change, while achieving commercial growth and profit targets.

Ian McNeil
Global Head of Customer Management
Risk Engineering
Zurich Insurance Company Ltd
T: +44 (0)77 1003 8416
E: ian.mcneil@uk.zurich.com

Kevin Parker is a highly experienced senior risk management and insurance professional, with over 40 years' experience of UK and EMEA insurance markets gained with Zurich Commercial Insurance. Mr Parker has a wide range of proven risk engineering, business development, customer relationship and project management skills. He has worked in various risk management areas, specialising in property and strategic risk with a track record of working with major global financial institutions, performing effectively at all organisational levels, effectively managing change in a constantly evolving risk landscape.

Kevin Parker
Head of customer Management (EMEA)
Risk Engineering
Zurich Insurance Company Ltd
T: +44 (0)78019 755 68
E: kevin.parker@uk.zurich.com

Reprinted from Risk & Compliance Magazine, July-September 2018 issue.

This document is intended for general information purposes only. While care has been taken to ensure the accuracy of the information, no entity member of the Zurich Insurance Group, including without limitation, in the United States, Zurich American Insurance Company, 1400 American Lane, Schaumburg, Illinois 60196; in Canada, Zurich Insurance Company Ltd, Canadian Branch, 400 university Avenue, Toronto, Ontario M5G 1S7; and outside the U.S.A. and Canada, Zurich Insurance Plc, Ballsbridge Park, Dublin 4, Ireland; Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zurich, Switzerland ('Zurich'); Zurich Australian Insurance Limited, 5 Blue Street, north Sydney, SW 2060, Australia and other legal entities, as may be required by local law, accepts any responsibility for any errors or omissions.

Zurich does not accept any responsibility or liability for any loss to any person acting or refraining from action as the result of, but not limited to, any statement, fact, figure or expression of opinion or belief contained in this document.

www.zurich.com