KRM22

Organisational Structures for Enterprise and Operational Risk

Response to the WFE Benchmarking paper

Document Type: Thought Leadership
Prepared by: Andrew Smart
Date: 21 August 2020

CONTENTS

Purpose

The purpose of this document is to provide a few constructive observations on the World Federation of Exchanges (WFE) Benchmarking Paper – Organisational Structures for Enterprise and Operational Risk published on February 12, 2020, and to contribute to the discussion and the WFE body of knowledge on the topics of Enterprise and Operational Risk.

The WFE Benchmarking Paper is available here: https://www.world-exchanges.org/our-work/articles/wfe-enterprise-risk-management-benchmarking-paper

Summary of finding

As stated in the press release accompanying the release of the WFE Benchmarking paper, the summary of findings were;

- On average, the dedicated enterprise risk function currently accounts for around 2% of a company's entire workforce.
- All the responding entities employ, as a base level, the three lines of defence model (with some labelling senior management or supervisors as an additional line):
    - First line of defence is the Executive (Group-level risk) Committee, whose primary responsibility is the day-to-day management of Risk;
    - Second line of defence is the Risk (management oversight) Committee, which incorporates the ERM function and is governed by the Chief Risk Officer. This line provides the risk universe and risk manager framework, ensures compliance, and reports up to the senior management team;
    - Third line of defence is the internal and external auditors who perform an independent assessment on the efficiency and effectiveness of the internal controls, risk management and governance.
- Internal audit (IA) forms an integral part of the third line of defence and the wider risk management structure. It is an independent function, performing regular reviews, providing oversight, and holding responsibility for risks, controls and governance assurance.
- Some firms have extended the model to include a 'fourth line of defence', reporting via bespoke committees or processes to their regulators. Further, some entities also designate the actions and roles of the senior management and board as distinct lines of defence and integrate those additional lines within the model.

Alongside this summary of findings, we believe it is worth highlighting the following statement made by Nandini Sukumar, Chief Executive Officer, WFE.

"*We found that WFE members are implementing sophisticated ERM practices right across their operations, which befits their status as national critical infrastructure. As ERM is an effective way of enhancing the resilience of exchanges and CCPs, it is imperative that all market infrastructures establish and operate the most advanced functions possible to ensure their resilience.*"

Evaluation

Resourcing

Within the resourcing section, the focus was on the level of resources devoted to enterprise risk management within exchanges and CCPs.

However, the paper could benefit from a discussion about the role of Chief Risk Officer (CRO). In particular, the paper does not indicate how many exchanges and CCPs have appointed a CRO, if appointed, where the CRO sits within the 'c-level' hierarchy and what their typical accountability lines are (reporting to CEO, CFO or Board Risk Committee?).

No comments were made on the level of resources or tools used to help improve the effectiveness of the ERM team.

Risk Management Model

The WFE study found that all the responding entities consistently use the three lines of defence model. This is entirely understandable, given the three lines of defence model is regarded by many within Financial Services as best practice.

it could be argued that this is driven primarily by firms seeking to meet regulatory expectations rather than a reflection of the value and effectiveness of this model. Indeed, there are often many questions about the value of this model as its practical implementation is not straight-forward.

One of the criticisms of the three lines of defence model is that rather than creating clarify, it creates confusion when implemented. Within the benchmarking paper, there is a hint that some exchanges and CCPs are experiencing this lack of clarity. There is mention of the fourth line of defence, and we suspect some of the participants would have implemented the concept of a 1.5 line of defence.

The mention that some entities use Risk Champions as part of their risk management approach is also evidence of the application of another widely used practice, often used to complement the three lines of defence model.

To address issues with the three lines of defence, specifically to bring clarity and embed accountability for risk management within exchanges and CCPs, I would recommend the use of the RACI model.

The RACI model has it originates in the programme/change management world however it has been used in other areas, including risk management. It can either compliment or replace the three lines of defence model. It is an easy to implement governance and decision-making model which clarifies an individual's role and authorities concerning a process or activity where ambiguities and uncertainty exist. It ties very effectively with regulatory Individual accountability regime approach. This RACI model is made up of four roles;

- Accountable (the buck stops here) – this is the individual who is ultimately accountable for the management of the Risk, who has decision-making authority over the Risk and makes the final decision about the management of the Risk. There is only one per item within the risk framework, Risk, control etc.

- Responsible (the doers) – these are the individuals who undertake the work to manage the Risk and implement the decisions taken by the accountable. There can be multiple responsible per item within the risk framework, Risk, control etc.
- Consult (keep in the loop) – these are the individuals who the accountable consults with prior to making decisions.
- Informed (keep in the picture) – these are the individuals who the accountable informs post making decisions.

The benefits of implementing RACI include greater decision-making transparency, faster decisions and a systematic streamlining of organisational decision-making processes.

Within the context of risk management, our experience shows that RACI has other benefits, including; it enables the risk team to 'speak the language of the business' and is a relatable approach as RACI is often already in uses within the firms. RACI also creates clarity and helps embed accountabilities for Risk at the individual level. This positively shapes culture and is aligned to the individual accountability regimes implemented or under consideration globally.

Enterprise Risk Management and Internal Audit Interaction

Within the WFE paper, there was a significant amount of excellent commentary related to the interaction between Enterprise Risk and Internal Audit. This links back to the consistent use of the three lines of defence model within exchanges and CCPs.

Risk Governance & the organisation of risk committees

The WFE paper states that exchanges and CCPs consistently have two to three layers of risk governance. This implementation of risk governance and the organisation of risk committees is as you would expect given the use of the three lines of defence model.

In discussing risk governance and the organisation of risk committees, there is a lack of clarity into what I would call the risk management 'drumbeat'. Do exchanges and CCPs operate their enterprise and operational risk management processes on a quarterly, monthly or real-time 'drumbeat'.

Across the industry, too often we see enterprise risk management processes in particular operating on a quarterly or monthly cycle, aligned to board and executive reporting timelines. This is often because of the high level of manual workload involved with enterprise risk management processes and heavy reliance on cumbersome spreadsheet 'systems'.

Within the risk governance section, there is an interesting sentence; "The risk parameters are delegated downwards, by the board, and should be embedded throughout an organisation".

The use of the phrase, "should be embedded" hints at a topic to be explored further; for example, how embedded are "risk parameters' within exchanges and CCPs?

This links to two points which I think this paper could have addressed in much greater depth;

1. Culture
2. Enterprise risk management drivers within exchanges and CCPs

Culture

One of the highest priorities to have emerged in the ten years since the 2008/2009 financial crisis has been the culture within the Financial Services industry. In the aftermath of the Financial Crisis regulators, boards and other stakeholders; including governments and professional bodies appear to have reached a similar conclusion; the culture of financial services was broken and needed to be 'fixed'.

The WFE paper does include this paragraph "As a general rule, the enterprise risk function will not own any specific risks – for instance, the management of credit risk – which is core to the function of a CCP. Instead, ERM is about maximising the consistency and effectiveness of risk management practices across the organisation. It is akin to making sure risk awareness and risk management practices are part of the DNA of the enterprise".

The use of the phase "DNA of the enterprise" captures the extent to which it is desirable to embed enterprise risk management into the exchanges and CCPs culture. Additionally, "tone from the top" is another phased which refer to firm culture.

However, in our view, the WFE paper could have had more value if it had provided some commentary around risk culture. In particular, how embedded and how 'lived' are enterprise risk management approaches and practices are within exchanges and CCPs? It is challenging to have a meaningful discussion about organisational structure without considering organisational culture.

Enterprise Risk Management drivers

Linking back to the use of the phrase "should be embedded", this paper does not clearly state what the key drivers for the adoption of Enterprise and Operational Risk within exchanges and CCPs are?

Is the adoption of more formal risk management approaches and structures driven by business needs? Is Enterprise and Operational risk management seen as a tool to drive value and create a competitive advantage? Or is it similarly been implemented to meet regulatory expectations?

Understanding the drivers of adoption will influence choices around organisation structure related to Enterprise and Operational Risk management.

Relationship between strategy and enterprise risk management

As we have already noted, there was good discussion about the interaction between enterprise risk management and internal audit. One area where this paper was lacking was a discussion about the interaction between enterprise risk and strategy within exchanges and CCPs.

The tone of the WFE paper is one where enterprise risk management is done for either defence reasons (risk minimisation) or regulatory reasons (what is expected).

We think it is fair to say that general discussion about enterprise risk management is shifting from a focus on minimising Risk to one where enterprise risk management is seen as having an important role to play in strategy execution and value creation.

Are exchanges and CCPs structuring Enterprise Risk Management as a risk minimisation function or a value creation functions or both? The benchmarking paper is silence on this topic.

Relationship between enterprise risk management and operational risk management

As a final point, the title of this WFE paper was Organisational Structures for Enterprise and Operational Risk. However, the paper itself was almost silence on operational risk management. Reference is made to it in the glossary where is defined as been part of Enterprise Risk Management along with financial Risk. Also, a Bank of England speech is referenced with the quote "operational risk management was under the spotlight as never before".

It is not unusual to use enterprise risk and operational risk interchangeably. However, to do so in a paper such as the WFE benchmarking paper is unfortunate, and we believe a missed opportunity. Clarifying and differentiating between enterprise risk management and operational risk management would have add value to the paper

It could have set out how these two different risk disciplines can be structured to add value individually but also aligned to together. It could have drawn attention to the different focus of these two different risk disciplines; where enterprise risk management related to firm strategy, business model, and create an enterprise-wide, aggregated view of Risk. In contrast, operational Risk is focused operationally; on processes, technology, change and people Risk.

Conclusions

The WFE Benchmarking paper – Organisational Structures for Enterprise and Operational Risk sets out the finding from the WFE's Enterprise Risk Working Group (ERWG) study into the organisational structures' exchanges and CCPs have implemented for Enterprise and Operational Risk.

We believe this paper makes a useful contribute to the enterprise and operational risk conversation within the membership of the WFE and we support many of the findings.

That said, we feel this paper would have benefited from a discussion about the CRO role and the role of organisational culture in delivering an effective enterprise and operational risk management. It is difficult to see why these two important points were missed out, given the topic of the paper.

Additionally, setting out clear definitions for enterprise risk management and operational risk management, and how these two risk management disciplines should work together would have been beneficial.

The WFE Benchmarking paper is timely and would encourage the WFE and its membership to continue to evolve and upgrade their thinking and use of enterprise and operational risk management.