WORLD FEDERATION OF EXCHANGES

A WFE Benchmarking Paper

Organisational Structures for Enterprise and Operational Risk

As Applied by Members of the World Federation of Exchanges

Enterprise risk management (ERM) functions and competencies are increasingly seen by market infrastructure providers as an effective way to enhance the resilience of exchanges and CCPs. As a first step to agreeing and harmonising industry ERM practices, the WFE's Enterprise Risk Working Group (ERWG) studied the way exchange and CCP operators structure their approach to risk management through such functional teams and their relationship with other parts of their organisations.

The study found that market infrastructures (MIs) are implementing advanced and embedded ERM right across their organisations which are tailored to deliver on the rigorous requirements and regulatory expectations applying to them as national critical infrastructure - something which distinguishes them from other parts of the financial system.

Introduction to the ERWG:

Risk management was originally associated with the use of insurance which evolved into financial risk management – involving the use of derivatives. Further onus has since been placed on the importance of risk management by regulation and business requirements over recent years. At the same time, ERM was developed as an answer to delivering a more structured, efficient, aligned and coordinated risk management methodology across business functions, to manage an organisation's (and its subsidiaries) full range of risks[1]. This strategy also adopts the concept that risk analysis, and management, should run throughout the entirety of an organisation. The ability to have a greater understanding of the resilience of an enterprise in the face of risks and (with the support of the ERM function) to manage that risk exposure, in a framework set by the board, realised via the use of ERM, helps to answer the needs that were set by said new regulations and emerging business risks.

International, regional and national financial services regulation and standards have rightly mandated requirements for market infrastructure to manage risk and implement appropriate measures. These requirements, alongside the need to ensure resilience and business continuity after incidents such as 9/11, for example, have seen exchanges and CCPs expand and improve ERM functions within their organisations.

The WFE's ERWG was established in June 2018, to connect Enterprise Risk Management (ERM) and Operational Risk Management (ORM) leadership and thinking at the world's financial exchanges and clearing houses. Membership is open to all exchanges and clearing houses who are full members of the WFE. The Working Group is mandated to forge best practices, codes of conduct and guidelines. It is also a vehicle for information sharing, education, awareness and benchmarking amongst its members. A particular objective of the group is to enhance and support board effectiveness and risk governance.

The ERWG commissioned, contributed to and oversaw this study.

[1]The Society of Actuaries, Chartered Enterprise Risk Analyst, Enterprise Risk Management (ERM), Fact Sheet, https://www.soa.org/globalassets/assets/Files/Newsroom/news-erm-fact-sheet.pdf

Methodology and Analysis:

This study is exclusive in its focus on exchanges and CCPs and their implementation of ERM.

In order to understand how exchanges and CCPs are implementing their ERM functions a survey of members of the ERWG was undertaken with a series of questions developed by leading ERM risk experts who operate market infrastructure. Risk managers responded from across twelve key jurisdictions around the world, representing a range of sizes and a combination of exchanges and CCPs. The results were collated and aggregated to enable average determinations of the responses to be made and leading examples of ERM implementation to be drawn out.

The focus of this piece is on organisational risk management roles and responsibilities. Whilst there are other measures, such as risk modelling, this is an important component to begin the discussion of risk management and naturally sits as the starting point in addressing enterprise risk. Implicit within the findings of the survey is the 'tone from the top' and the priority and value given to risk management in how the board and senior management engage with their risk managers. This has implications for the risk culture of an organisation more broadly. Firms also use, and are currently adapting, a variety of methods to incentivise and promote the importance of risk management from the bottom up, e.g. through their risk and control self-assessment (RCSA) or equivalent process or through direct linkage of staff's objectives in their appraisals, mandatory training and other mechanisms.

It is clear from the results of the study that a well-developed ERM function should, in turn, help to inform and help to guide management and board level decision making. Further, risk management is an integral part of any business's activities, especially that of financial services companies. The risk appetite of a company defines how much risk the company will accept and it then needs to decide which risks it makes sense to mitigate; which to transfer out; and which to reject [avoid][2]. Good risk management helps to reduce the likelihood and mitigate the impact of negative outcomes and help companies take advantage of positive ones[3]. It also provides boards/management with a base understanding of what could prevent the company from achieving its strategic and business objectives[4].

[2] McKinsey and Company, A Board Perspective on Enterprise Risk Management, February 2010, https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/18_a_board_perspective_on_enterprise_risk_management.ashx
This article was originally published by McKinsey & Company, www.mckinsey.com. Copyright (c) 2019 All rights reserved. Reprinted by permission.

[3] McKinsey and Company, Making Risk Management a Value Added Function in the Boardroom, September 2008,https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/Risk/Working%20papers/2_Making_risk_management_a_valueadding_function_in_the_boardroom.ashx
This article was originally published by McKinsey & Company, www.mckinsey.com. Copyright (c) 2019 All rights reserved. Reprinted by permission.

[4] PwC, How your board can ensure enterprise risk management connects with strategy, April 2017, https://www.pwc.com/us/en/governance-insights-center/assets/pwc-how-your-board-can-ensure-enterprise-risk-management-connects-with-strategy.pdf

5

The ERWG believes it is particularly important to be clear in communicating what the industry is already undertaking in the measures taken in the management of risk to its stakeholders. This is to ensure that the sector can inform and give assurance of the increasing priority industry has attached to this evermore crucial aspect of a financial services' functions. For example, in a recent speech on operational resilience, Nick Strange, the Director of Supervisory Risk Specialists at the Bank of England, stated that operational risk management was under the spotlight "as never before"[6] as it is considered key to the Bank's mission of maintaining market stability.

The Bank of England advised that it is the use of effective risk management which enables the desired outcome, in that case, of operational resilience. International standards setters such as IOSCO, the Financial Stability Board and others will no doubt continue to scrutinise the role of risk management in financial services.

As critical national infrastructure, exchanges and CCPs are likely to be at the forefront of this increasing scrutiny. The ERWG represents organisations which have implemented dedicated resource and governance structures, in the manner outlined in this paper, to ensure that exchanges and CCPs are ahead of the curve and lead in their practices to counter risk and inform future policy.

[5] Exhibit from "Transforming enterprise risk management for value in the insurance industry", July 2016, McKinsey & Company, www.mckinsey.com. Copyright (c) 2019 McKinsey & Company. All rights reserved. Reprinted by permission.

[6] Bank of England Operational Resilience – a progress report, Speech by Nick Strange, May 2019, https://www.bankofengland.co.uk/speech/2019/nick-strange-operational-risk-europe-conference

In this paper the WFE sets out the key themes and questions any market infrastructure operator needs to consider when reviewing their organisational structure to address the management of risk. This paper details how, in aggregate, these institutions are implementing their risk structures. It reflects upon (but does not seek to cover details) the use of established tools including KRIs, risk modelling, identification of risk, risk appetite and encompasses enterprise risk management rather than purely operational risk. Specific issues such as cyber risk/resilience are also not exclusively dealt with in the paper but are an ever-increasing focus for consumers and regulators and something which is being addressed by the WFE's cyber-security working committee – *GLEX*.

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 WFE and its members regard enterprise risk management as an evolving field, corresponding with other variations of risk practices, which are also evolving.

WORLD FEDERATION OF EXCHANGES

Glossary of terms	
ERM (Enterprise Risk Management)	As defined by the Committee of Sponsoring Organizations of the Treadway Commission[7], deals with risks and opportunities affecting value creation or preservation. It can be defined as follows: *Enterprise risk management is "the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value."*[8] ERM encompasses the managing of both financial and operational risk (including the risks related to internal processes, systems, human behaviour and other aspects of the organisation). Other relevant risks can be related to compliance with laws, regulations and ethical standards (compliance risk), environmental risk etc. as well as the handling of external risk factors such as, for example, political risk, macroeconomic factors or catastrophic scenarios. [9]
ERM function	A centralised risk management function is responsible for establishing and maintaining the risk management processes, with day-to-day responsibility for collating and consolidating risk monitoring, measurement and evaluation information for reporting to management/board. It provides the organisation with a formal risk management framework, including the 'risk universe' and the risk appetite with thresholds, and appropriate training programmes aimed at improving the risk management culture and promoting common risk terminology and concepts applicable to the whole organisation.

[7] Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management — Enterprise Risk Management Integrating with Strategy and Performance, 2017, https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

[8] For the purposes of clarity in this document dedicated roles with responsibility for ERM will be referred to as 'ERM functions'.

[9] Guidelines for the Risk Management function, IIA Norge, 2017, https://iia.no/wp-content/uploads/2017/05/2017-Guidance-for-the-Risk-Management-Function.pdf

WORLD FEDERATION OF EXCHANGES

ERMF (Enterprise Risk Management Framework)	An integrated framework of responsibilities and functions driven from the governing body down to operational levels which identifies, quantifies, and manages the risks of the business[10]. Additionally, CPMI-IOSCO's has defined this as "An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks…An FMI should have risk-management policies, procedures, and systems that enable it to identify, measure, monitor, and manage the range of risks that arise in or are borne by the FMI. Risk management frameworks should be subject to periodic review." (CPMI-IOSCO Principles for Financial Market Infrastructures[11]) The framework is set by the Risk Committee, approved [and reviewed] by the board, for the identification, assessment, reporting and management of risks. A framework for risk management will typically include the following elements[12]: • Identification of internal and external matters which influence an enterprise's achievement of objectives • Determination of risk appetite and risk management policy • Design of the risk management function and organisation as well as areas of responsibility • Establishment of internal and external communication and reporting structures • Allocation of resources to the function Some examples of international risk management framework standards are: o ISO 31000:2018 - Risk Management – Guidelines o COSO: 2017 Enterprise Risk Management - Integrating with Strategy and Performance
Three Lines of Defence	90% of members used the three lines of defence model of risk management**.** The model distinguishes between three groups (or lines) that are involved in internal control and risk management: • Functions that own and manage risk (first line) • Functions that exercise oversight over risk (second line) • Functions that provide independent assurance (third line)[13]

[10] Coopers & Lybrand, Generally Accepted Risk Principles ("GARP"), 1996, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD78.pdf
[11] CPMI-IOSCO Principles for Financial Market Infrastructures, April 2012, https://www.bis.org/cpmi/publ/d101a.pdf
[12] Ibid, Guidelines for the Risk Management function
[13] Guidelines for the Risk Management function, IIA Norge, 2017, https://iia.no/wp-content/uploads/2017/05/2017-Guidance-for-the-Risk-Management-Function.pdf

WORLD FEDERATION OF EXCHANGES

	Broken down this includes: 1. The first line of defence (Management/business functions) – operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks. 2. The second line (Risk Management and Compliance functions) are the functions which oversee or specialise in risk management and compliance who facilitate the implementation of effective risk management practices and reports to the Board Committees on risk exposure [crucial in the prioritisation of Business as Usual operations or change programmes in providing initial assurance to management and the board]. 3. The third line (Internal Audit/External assurance providers) is an independent internal audit function will, through a risk-based approach to its work, provide [in-depth] assurance to the organisation's board of directors and senior management. This assurance will cover how effectively the organisation assesses and manages its risks and will include assurance on the effectiveness of the first and second lines of defence. It encompasses all elements of an institution's risk management framework and all categories of organisational objectives[14].
Risk appetite	Risk appetite is defined as the level of risk that an entity is prepared to accept in pursuit of its strategic objectives. This may result in a formal statement of risk appetite.
Controls assurance	The manner in which an organisation has surety that its risk policies are being implemented, through internal and external audit.
Operational resilience	The ability of firms, [F]MIs and the sector as a whole to prevent, detect, respond to, recover and learn from operational disruptions[15].

14 Chartered Institute of Internal Auditors, https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/

15 Bank of England Operational Resilience – a progress report, Speech by Nick Strange, May 2019, https://www.bankofengland.co.uk/speech/2019/nick-strange-operational-risk-europe-conference

The Responding Entities

The responses covered **twelve institutions**, ranging in both their size and their market infrastructure (MI) – exchanges and clearing houses. There is a uniformity in the core structures applied to the management of organisational risk which naturally develop in accordance with the complexity and practices of the MI, as well as in the size of the organisation.

Results of the Study

Via Q and A on Organisational Risk Structure

Resourcing

What is appropriate dedication of staffing to the enterprise risk function?

The term 'Risk function' is open to interpretation – some organisations include financial and non-financial risk, inclusive of operational and technology risk, inclusive of some specific risk management teams such as cyber. However, the bespoke ERM function is often small in scale and takes a coordinator and facilitator role in collaboration with other associated risk roles.

Employing a broad definition of ERM; on average the ratio of risk function to the size of a company's entire workforce is currently around **2%** dedicated to ERM functions.

This is based on a range of 0.2 - 4.1%.

Risk Management Model

What models of risk management are operating across MIs? Who carries out the functions of risk management?

The *three lines of defence* model is consistently used by all the responding entities. There is a common understanding of the terms and application of the model (see glossary of terms for definition and design).

The model is one which will evolve and new incarnations are being developed. However, the current model is dominant but there are some notable emerging adaptions to it, especially regarding an expansion of the third line, sometimes termed a 'fourth line of defence', which is a model that endows supervisors and external auditors (who are formally outside the organisation) with a specific role vis-à-vis the internal control system[16]. The application of external auditors as opposed to internal, could arguably be symptomatic of the growing requirements and behaviours of regulators, as well as the nature of their interaction with financial services. Further, some entities may also designate the actions and roles of the senior management and board as additional, distinct, lines of defence and integrate those additional lines within the model.

MIs generally operate the following application of the model:

[16] BIS, The "four lines of defence model" for financial institutions, 2015 https://www.bis.org/fsi/fsipapers11.pdf

- In effect the first line of defence includes all employees (sometimes with risk coordinators) being accountable for undertaking, day-to-day monitoring and reporting risks to their business operations.

- The second line of defence is the risk management oversight, incorporating the ERM function, (governed by the Chief Risk Officer), providing the risk universe and the risk management framework, direction, ensuring compliance and assessment for internal controls on the first line and reporting up to senior management/board.

- The third line of defence is the internal and external auditors who perform an independent assessment on the efficiency and the effectiveness of the internal controls, risk management and governance to provide assurance and consultation for the board of the company.

The mechanisms by which this happens are detailed in the risk governance discussion below. Some entities use 'risk champions', often representing regional parts of an entity, who hold responsibility for reporting of risk within their units and for driving ERM processes of the company.

Risk Governance

What is the Risk Governance structure employed by MIs? (i.e. how are risks reported up to the Board? Is there a dedicated Risk Committee? How often do they meet?)

The size, scope and longevity of an organisation impacts the sophistication and depth of its risk governance arrangements. In order for a large institution to understand the risk exposure of all the parts of its organisation, it is necessary to have procedures in place that streamline the information to a very senior management group who oversee the whole entity's risk management. Smaller institutions do not have such evolved practices but arguably can have an equal understanding of the risk management without intricate structures because of their smaller scale of operations.

All responding organisations consistently had two to three layers of governance relating to the management of risk. There is an executive risk committee, made up of the individual leads of the group's functions, (covering other first line risk related committees and business operations reporting their risk) which meets frequently and is responsible for 'dashboard' risk profiling and KRIs, to ensure the day-to-day management or mitigation of risk in order to remain within the company's risk appetite limits.

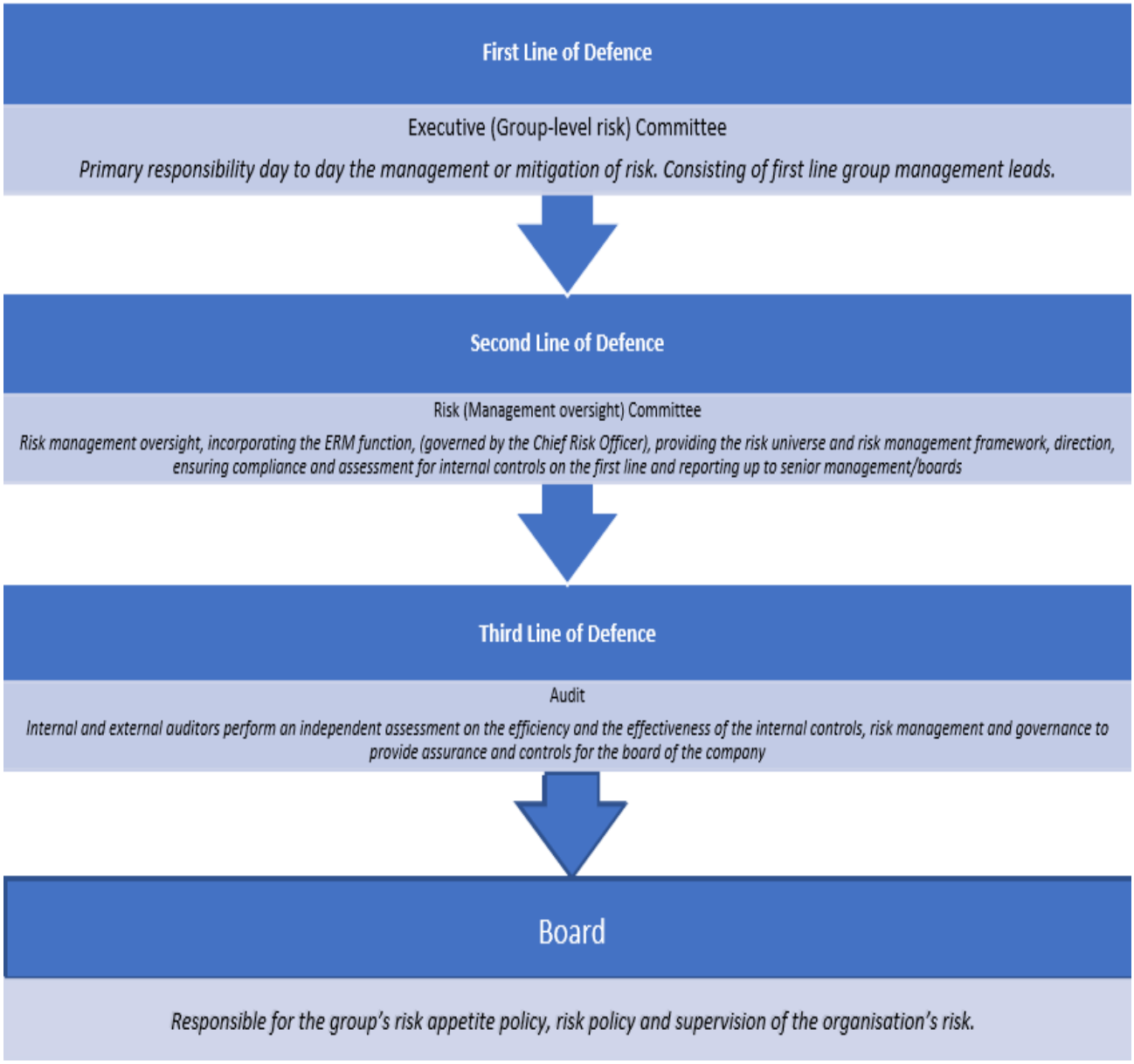
Second is a risk (management oversight) committee which is generally appointed by, or a subset of, the board to oversee the quarterly reporting and exists to ensure compliance with risk management approach/principles, risk policy (limits) and framework. It governs the ERM. Most risk committees meet on a quarterly basis, unless there are urgent issues to address. The function should also be able to provide ad hoc reporting to the board as and when required.

The third is in the form of an audit committee who have overall sight of the risk management profile and, combined with the risk management committee, assess the effectiveness of the company's risk management and internal controls. This committee reports to the Board.

Ultimately the board is responsible for the group's risk appetite policy, risk policy and supervision of the organisation's risk universe. The risk parameters are delegated downwards, by the board, and should be embedded throughout an organisation.

These structures run parallel and form the mechanisms by which the three lines of defence model operates.

Risk Governance Flow Chart



In line with the 'fourth line of defence' (not depicted in diagram), some entities operate external regulatory committees between national market regulators and key interlocutors or at least submit information on formalised basis.

Internal Audit – Assurances

Does a company's internal audit hold responsibility for controls assurance and testing?

Internal audit (IA) forms an integral part of the third line of defence and the wider risk management structure. This is realised via an independent function, i.e. internal audit, performing independent reviews on a regular cycle. The IA provides independent oversight and holds responsibility for risks, controls and governance assurance.

IA and ERM – What's the difference?

Does the ERM function also provide controls assurance for the company? Does this entail the use of 'controls testing'? How does this relate to the IA function?

Under the second line of defence, the ERM may provide control assurance around process and controls design in high risk areas, in line with the risk profile and risk appetite identified by the board/risk management committee. The IA function performs an independent verification or review on this control assurance and should have an important collaborative relationship to ensure efficiency.

In practice the ERM function provides oversight of controls through approaches such as 1st line self-assessments, often based upon a defined sampling methodology to assure that the controls are working and performs deep-dive reviews as appropriate and guided by the Risk Committee. IA uses the reports of this testing to inform their own testing programmes and ensure independent control and oversight over the process.

IA and ERM – Who does what? **In what form are the controls assurances organised and prioritised to provide adequate organisational coverage?**

The associated business process/service criticality will dictate the frequency and priority attributed to it by IA, under an audit plan – overseen by the Audit committee. This will often take the form of all auditable areas of business being reviewed at least every three years, two years for those themes, business functions, systems or project deemed to present more of a risk to the business and every year for those representing the highest inherent risk.

There is often a collaborative split in the focus of the work between ERM and IA to avoid overlap.

ERM Parameters

How are a company's enterprise risk functions formalised? What do the Terms of Reference (ToRs) look like?

Rather than a ToR, there is an ERM policy, or it is held within the risk framework, which is mandated to ERM functions by the risk management committee or the board itself, which outlines the roles and responsibilities of the ERM/three lines of defence.

Regulatory Engagement

Does the regulator or supervisory authority oversee an entity's ERM?

The manner in which an entity reports to a supervisory authority varies between jurisdiction. Those who operate a 'four lines of defence' or enhanced third line of defence, will report via bespoke committees or processes to their regulators. Others have set reporting periods, of which those reports may take place on multiple levels of a company's functions. Regulators attention on ERM has reportedly increased substantially and there is a growing expectation that major initiatives or changes to risk areas have been processed through all internal governance structures (via the three lines model) before they are submitted for regulatory approval.

WFE and ERM – *Where to next?*

As stated at the start of this paper, ERM is growing in its reach and use, given the resulting value associated with resourcing such a function, in an age of ever-growing risk management requirements. The purpose of this paper is to form the foundation of how market infrastructures are establishing and directing their ERM functions. The ERWG will be conferring with its membership and collaborating with regulators and policymakers in scoping out the landscape of how they should evolve their functions to further address emerging issues. The ERWG has already identified and begun its analysis on the use of KRIs, development of risk appetite frameworks and other risk related topics. To enable future benchmarking or best practice information sharing, the ERWG will also be undertaking future reviews of its positioning, adaptations and alterations on the subject of this paper, as well as other best practice elements of risk management.

If your organisation wants to contribute to the delivery of benchmarking or best practice papers and analysis for the industry, please contact the WFE to find out more about membership.

For further information:

Jonathan Pallant, Regulatory Affairs Manager, jpallant@world-exchanges.org

Richard Metcalfe, Head of Regulatory Affairs, rmetcalfe@world-exchanges.org