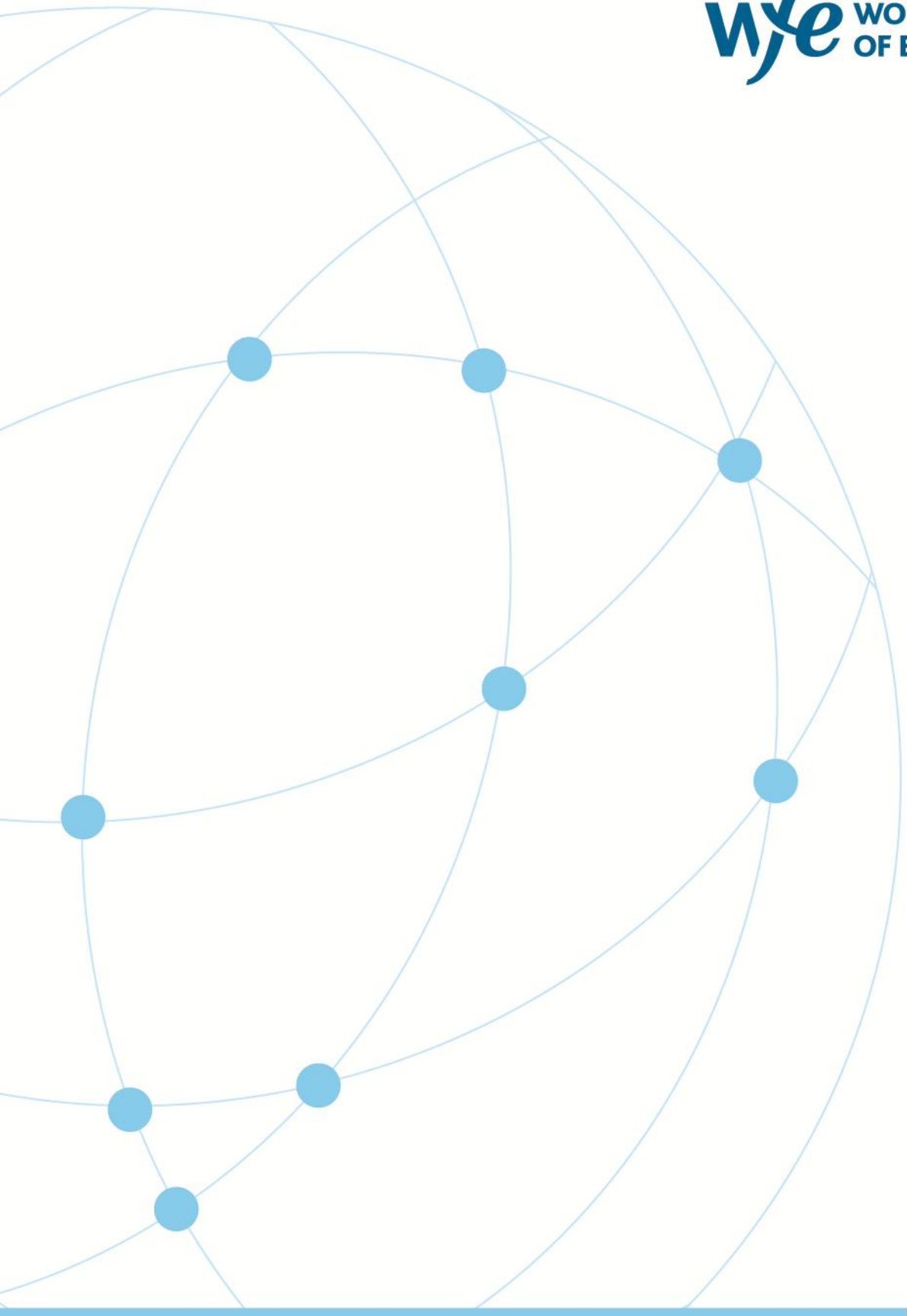
WORLD FEDERATION OF EXCHANGES



Top Risks Identified Across WFE Membership – 2025 Insights

January 2026

Background

Established in 1961, the WFE is the global industry association for exchanges and clearing houses. Headquartered in London, it represents over 250 market infrastructure providers, including standalone CCPs that are not part of exchange groups. Of our members, 37% are in Asia-Pacific, 44% in EMEA and 19% in the Americas. WFE's 87 member CCPs and clearing services collectively ensure that risk takers post some $1.3 trillion (equivalent) of resources to back their positions, in the form of initial margin and default fund requirements. WFE exchanges, together with other exchanges feeding into our database, are home to over 51,000 listed companies, and the market capitalisation of these entities is over $110 trillion; around $140 trillion (EOB) in trading annually passes through WFE members (at end 2024).

The WFE is the definitive source for exchange-traded statistics and publishes over 350 market data indicators. Its free statistics database stretches back more than 40 years and provides information and insight into developments on global exchanges. The WFE works with standard-setters, policymakers, regulators and government organisations around the world to support and promote the development of fair, transparent, stable and efficient markets. The WFE shares regulatory authorities' goals of ensuring the safety and soundness of the global financial system.

With extensive experience of developing and enforcing high standards of conduct, the WFE and its members support an orderly, secure, fair and transparent environment for investors; for companies that raise capital; and for all who deal with financial risk. We seek outcomes that maximise the common good, consumer confidence and economic growth. And we engage with policymakers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in a globally integrated financial system.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

Chhavi Sinha, Regulatory Affairs Manager: csinha@world-exchanges.org

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

Or

Nandini Sukumar, Chief Executive Officer: nsukumar@world-exchanges.org

Top Risks Identified Across WFE Membership – 2025 Insights

Enterprise Risk Working Group Annual Assessment

Executive Summary

The World Federation of Exchanges (WFE) conducted its annual assessment of risk through the Enterprise Risk Working Group (ERWG), between July and August 2025. The survey gathered anonymous responses from 29 member firms globally. Members ranked risk categories from 1 (least important) to 5 (most important), providing qualitative insights as well.

While cyber resilience remains the top concern among enterprise risk professionals, it is also part of a wider concern about digital resilience. The top risks identified reflect growing concerns around digital resilience, AI integration, and regulatory complexity. Cybersecurity continues to rank highest, closely followed by technology-related and operational risks (including process failures and human error).

The WFE and its members use this information to inform their own approach. For the WFE, we use this information to focus activities on the key risks members identify. For our members, they use this information to benchmark their views against their peers and inform strategic discussions. We share this information more broadly with policymakers and the ecosystem with the hope that it is similarly useful for them.
While these results are consistent with topics discussed within the ERWG over this and previous years, we note that this is not a collective exercise, and the exact ranking and emphasis may vary considerably from member to member.

Regional & Functional Insights

Respondents represented a diverse mix of market functions and regions. The breakdown by region was:

- EMEA: 48%
- APAC: 28%
- Americas: 24%

We surveyed the exchange groups and the three key MI functions shared by the respondents covered, namely equity exchanges, derivatives exchanges and clearing Houses

Key Findings

Weighted Survey Results

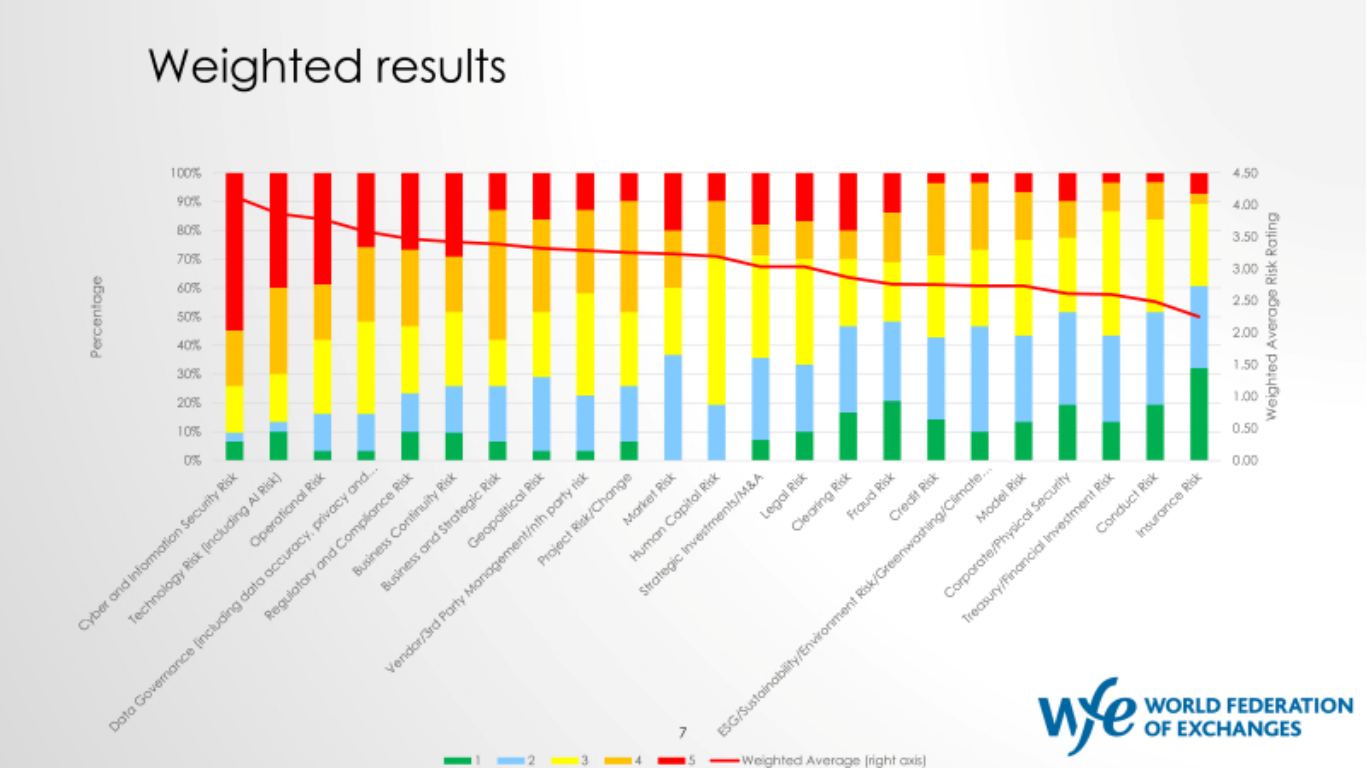


Figure 1: Weighted Survey Results

The above slide shows the weighted survey results for each risk category by combining how respondents scored risks from 1 (least important) to 5 (most important). Each bar displays the proportion of responses at each score, while the red line shows the weighted average—meaning risks with more "5" ratings naturally rank higher. In simple terms, the weighted average turns all the different responses into one summary number, making it easier to compare the importance of risks across the dataset.

Key Risks

Cyber and Information Security Risk, Technology Risk (including AI), and Operational Risk are the key risks identified by WFE members. These three risks were identified as the number one risk more than any others. Furthermore, the weighted average shows broad consensus that they are priority risks. This reflects the strength of feeling from our members. It is also consistent with previous years where these risks have featured prominently.

Figure 2: Risk Trends Over Three Years

Cybersecurity remains the top concern due to persistent and increasing threats, as noted by financial regulators[1] but also more broadly[2], and its potential to undermine market integrity and financial stability. A successful cyberattack on an exchange can clearly **disrupt trading.** However, as demonstrated by the Ion Trading ransomware attack in January 2023, cyberattacks on widely used platforms like Ion can cause extensive disruption that extends far beyond the control of the exchanges forced to respond.[3]Risk is therefore amplified by complex systems and interdependencies within the financial system.

Closely linked to the next identified key risk, threat actors are becoming more sophisticated with improvements in technology. AI-driven attacks are increasingly used. Furthermore, the prospect of **Quantum Computing** poses an emerging high-impact risk to encryption and fraud detection systems.
The growing inability to secure cyber insurance, even against remote but impactful events, poses a threat to market confidence and recovery.

Technology risk, especially with AI adoption, introduces new vulnerabilities and ethical considerations. While AI brings numerous benefits to financial services, [4] the exchange and CCP industry is cognizant of the importance of managing potential risks, ensuring that AI applications align with ethical and regulatory standards, and establishing a foundation

[1] For example, recently, *the SEBI Chairman, Shri Tuhin Kanta Pandey remarked that Cybersecurity threats have the potential to create systemic disruptions. As market participants increasingly rely on third-party service providers and cloud-based platforms, new vectors of risk emerge —sometimes beyond traditional regulatory perimeters.*
[2] For example, the World Economic Forum's Annual Meetings of the Global Future Councils and Cybersecurity
[3] CFTC comments on ION Cleared Derivatives issues after Russian-linked hack CFTC Comments On ION Cleared Derivatives Issues After Russian-linked Hack - FinanceFeeds
[4] The WFE, 31st October 2024: The Role of Artificial Intelligence in Shaping the Future of Exchanges & Clearing Houses: Opportunities, Challenges, and Regulatory Principles

for the responsible use of AI in the financial sector. Exchanges and CCPs are valued trusted parties operating under stringent regulatory frameworks. Financial institutions are currently effectively using existing risk management frameworks to manage AI risks. In many ways some AI risks are similar to more traditional risk.

Operational risk refers to the possibility of loss resulting from **failures in internal processes, people, systems, or external events**. It arises from the **day-to-day functioning** of an organization — for example, system outages, human errors, fraud, or external disruptions such as natural disasters or cyberattacks. Exchanges recognise their responsibilities in effectively addressing a market outage/other events and therefore, have well-defined outage playbooks, thresholds for inactivity, and disaster recovery measures and strategies to manage disruptions effectively. Financial markets and exchanges depend on highly automated, interconnected systems where even minor disruptions can have **wide-reaching impacts**. Increasing reliance on **digital platforms, AI, and cloud infrastructure** could complicate risks to cyber incidents, and third-party risks. Events such as **pandemics, geopolitical crises, or natural disasters** can severely disrupt business continuity. Operational risk persists because **no system or process can completely eliminate human error, technology failure, or external disruption**.

Moderate Risks

In the middle, risks such as Business Continuity and Strategic Risk, Market Risk have averages around 3. This indicates mixed perceptions – important, but not universally seen as critical. Other notable risks include: **Data governance risk** is closely linked to the AI risk – the model is only as good as the data. In addition, data governance also relates to the continued importance of privacy.

- Over the years, **Regulatory risk** shows volatility, reflecting shifting global policy landscapes and resultant compliance challenges. Regulatory risk tends to fluctuate over time because financial institutions operate in an environment where global rules and expectations change frequently. For example, the introduction of the Digital Operational Resilience Act (DORA) in the EU significantly raised compliance obligations for ICT and cyber resilience, requiring firms to redesign internal processes, enhance incident reporting, and adapt to new oversight structures. These waves of regulatory change can cause volatility in how organisations perceive regulatory risk: when major new rules are introduced or existing ones are revised, the perceived risk spikes; once firms adjust and compliance stabilises, the perceived risk typically declines until the next regulatory shift emerges.

- **Vendor/3rd Party Risk**: Dependence on **shared technologies** (e.g., cloud, APIs, market data feeds) increases exposure to **third-party or supply-chain risks**. Financial institutions, like other businesses, engage third-party providers to support critical functions including technology, legal, and data management services. As highlighted in WFE's 2023 response to the FSB consultation on third-party risk[5], such engagements can be both a source of risk and a risk management tool. For instance, third parties may be leveraged to enhance cybersecurity testing, complementing the institution's own efforts, thereby helping to manage operational and technology risks more effectively.

- **Geo-political Risk:** While the direct impact of geopolitical events—such as sanctions, trade tensions, or regional conflicts—varies across jurisdictions, the high risk score indicates that members are broadly concerned about uncertainty and instability in the global environment. Even if a specific event does not affect their operations directly, geopolitical developments can create ripple effects on markets, regulations,

[5] The WFE response to FSB consultation on – enhancing third-party risk management and oversight (August 2023)

and supply chains, prompting caution and nervousness among institutions. In short, the elevated score reflects a general perception of risk and heightened vigilance, rather than uniform exposure across all members.

Residual Risks

Lower-ranked risks should not be dismissed, but it's clear that members see them as secondary priorities relative to cyber and technology risks. Toward the lower end, we see categories like Conduct Risk and Insurance Risk, which scored below 2.5. These appear to be viewed as less pressing compared to others.

- **Conduct Risk:** Unethical or unlawful actions can harm clients, investors, or market integrity, potentially resulting in regulatory sanctions, reputational damage, and reduced stakeholder trust.
- **Insurance Risk:** Increasing cyber, technology, and operational exposures are making coverage harder to obtain and more costly, leaving firms more vulnerable to significant losses.

Conclusion

This weighted average approach gives us a clearer picture of consensus across the industry – not just which risks are mentioned most, but how strongly members feel about them.

The WFE is actively using this information to focus on the most important risks identified by our members. We will use our working groups as forums to discuss these topics, encourage the sharing of best practice and this will guide our discussions on where to focus our collective efforts.

Our members are well aware of the above risks and their potential implications. To address them, WFE members convene quarterly through various Working Groups — including the Global Exchange Cybersecurity Working Group (GLEX), the Technology Working Group (TWG), and the Enterprise Risk Working Group (ERWG). These groups comprise Chief Information Security Officers (CISOs), Chief Technology Officers (CTOs), and Chief Risk Officers (CROs) from stock exchanges and CCPs worldwide.

The Working Groups provide a platform to share insights on emerging cyber threats and technologies observed across jurisdictions. They also collaborate to develop best practices and conduct benchmarking exercises on key topics such as cybersecurity resilience (including ransomware and quantum computing preparedness), third-party risk management, identification of emerging risks, and AI governance and use of AI; Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs).

Appendix

Survey Methodology:
Members ranked risk categories from 1 (least important) to 5 (most important). Weighted averages were calculated to determine the top risks. The survey was conducted anonymously using a secure survey tool.