FERMA
Federation of European Risk Management Associations

29 June 2017

FERMA calls for cyber risk governance groups led by risk managers to increase organisations' resilience to developing threats - new report

European risk experts have called for organisations to create dedicated internal cyber risk governance groups to address digital risks across the whole enterprise as the threats evolve. The recommendation for a cyber risk governance model comes in a report published today (June 29) by the Federation of European Risk Management Associations (FERMA) and the European Confederation of Institutes of Internal Auditing (ECIIA).

FERMA and ECIIA presented their report at a high-level event at the European Parliament with representatives of the EU institutions, the World Economic Forum, risk and audit practitioners from European businesses, and other European stakeholders.

The report, *At the junction of corporate governance and cybersecurity*, aims primarily at supporting European organisations in meeting their obligations under the EU General Data Protection Regulation and Network Information Security Directive. Recent cyber attacks, however, increased concerns on what the risk experts see as a wider lack of focus on risk governance in cyber security.

The President of FERMA Jo Willaert states, "***As recent attacks show, cyber risk is an enterprise issue that affects strategic aspects of the board's mandate including valuation, reputation and trust. The management of cyber risk has, therefore, become a corporate issue that should be reflected in the governance of the company.***"

He adds, "***Our two professions are joining forces on cyber risk management by exchanging information on the ERM system and the cyber controls in place, ensuring that mitigation plans are auditable from their conception. This is crucial to evaluate their impact and review the alignment with the strategy.***"

The report calls for the creation of cyber risk governance groups, chaired by the risk manager, to operate across functions within the enterprise. The role of the group is to determine the potential cost of cyber risks across the whole organisation, including catastrophic risk scenarios, and propose mitigation measures to the risk committee and the board.

In addition to the risk managers, the group is to be composed of representatives of all key functions at an enterprise level involved in digital risk, notably IT, human resources, communications, finance, legal and the data protection officer (DPO) and chief information security officer (CISO). Internal audit will provide the necessary assurance to the board that the cyber risk controls are operating effectively.

Adds Jo Willaert, "***Our recommended cyber risk governance model constitutes an innovative way for organisations to approach cyber security. It will allow the board of directors to demonstrate that cyber risks are managed on a rational and documented analysis of the risks across the organisation.***"

The full report "*At the Junction of Corporate Governance & Cybersecurity*" is available on the FERMA website at http://bit.ly/2rfKtRv

Notes to editors

The FERMA-ECIIA cyber risk governance model is anchored in two strong sets of principles: the eight principles set out in the OECD's Digital Security Risk Management

recommendation (2015) and the Three Lines of Defence model, recognised as a standard of Enterprise Risk Management (ERM)."

FERMA-ECIIA Cyber Risk Governance Model
Based on Three Lines of Defence

MEDIA CONTACTS
Ms Typhaine Beaupérin, FERMA CEO: typhaine.beauperin@ferma.eu
tel: +32 (2) 761 94 31
Lee Coppack, FERMA Media coordinator: lee@coppack.co.uk
tel: +44 208 318 0330/ +44 7843 089904

All FERMA press releases can be found here

About FERMA
FERMA - The Federation of European Risk Management Associations - brings together 22 national risk management associations in 21 European countries. FERMA represents the interests of over 4800 risk and insurance managers in Europe active in a wide range of business sectors from major industrial and commercial companies to financial institutions and local government bodies. More information can be found at www.ferma.eu