



Response to the European Commission consultation on non-financial reporting guidelines

15 April 2016

Executive Summary

The Federation of European Risk Management Associations (FERMA) welcomes the opportunity to contribute to the Commission consultation on non-financial reporting guidelines, following article 2 of Directive 2014/95/EU on disclosure of non-financial and diversity information by certain large undertakings and groups.

FERMA represents the interests of more than 4700 European risk and insurance managers, of whom a large majority work in companies that are within the scope of the Directive¹. Risk managers play a crucial role within their organisations with respect to the management and treatment of complex risks and insurance issues.

FERMA urges the Commission to recognise in its guidelines the fundamental role of risk managers and the value of Enterprise Risk Management (ERM) methodology in the reporting of non-financial elements.

The ERM approach works in conjunction with a deep understanding of the business model of the organisation. It is a pre-condition to identify the principle risks connected with the elements of Corporate Social Responsibility (CSR) to be reported and then consider how they can be mitigated. In that respect, FERMA also understood that what is commonly called Corporate Social Responsibility (CSR) is just one of the many non-financial risk factors to be considered.

FERMA strongly believes that reporting the risks connected with CSR elements goes far beyond concern for reputation management. Being in control of these risks opens the way for productivity and efficiency gains over the long term. This will apply especially in areas like energy and raw materials consumption, workforce stability and performance, and the capacity to create new markets for new products and services.

When it comes to reporting these risks on an enterprise basis, it will be difficult for specialists in each department to connect different aspects of risk across other functions, leaving grey areas where reporting may be incomplete. Yet, one missed element can result in fines, legal costs,

¹ According to FERMA 2014 European Risk & Insurance report carried out among 850 risk professionals, 83% of respondents work in organisations with over 1.000 employees and 78% in organisations with a turnover of more than 100 million Euros (<http://www.ferma.eu/app/uploads/2014/10/20140828-FERMA-2014-Presentation-FINALE-FINALE.pdf>)



loss of contracts, personal injuries... and, thus, cost the organisation its reputation and impact it financially.

Organisations need to be assisted in this new process of reporting risks linked to non-financial information. Risk reporting is a key element of the risk manager's role. Because of the cross-functional nature of the risk manager's mission, he or she is the best placed person in the organisation to provide assurance that the various types of risks, including CSR, faced by an organisation have been identified and managed.

This reporting contains an analysis of risks connected to the non-financial elements and a response to them. The choice of methodology is crucial and should facilitate the disclosure by making it understandable, reliable and comparable.

The benefit of having risk managers in charge of this risk reporting is that it makes it possible to validate the strength of the organisation's response to these threats. Reporting on these risks cannot be limited to the financial impact.

FERMA strongly supports the idea that companies should take a sustainable and long-term strategic approach to their businesses. FERMA has always promoted consideration of the full range of risks, allowing the board and top management to properly set their risk appetite according to the full scope of possible impacts and to prepare a suitable response, such as mitigation plans².

The creation of a complete, company-wide risk management policy, including non-financial aspects, that leads to thorough risk knowledge should be seen as a global decision-making tool for the board.

² See FERMA 2013 position paper in on the proposed non-financial reporting Directive 2013/34 <http://www.ferma.eu/blog/2013/06/ferma-position-paper-on-the-proposed-directive-on-disclosure-of-non-financial-and-diversity-information-by-certain-large-companies-and-groups/>



I. General principles and key attributes of the non-financial information

Q1 What aspects of disclosure of non-financial information do you think that should be addressed by the GUIDELINES?

The guidelines should promote a **common risk management language** throughout a company or a group. The guidelines should help organisations to report their risks connected to non-financial elements using the ERM methodology defined as a process “*designed to identify potential events that may affect the entity, manage risk to be within its risk appetite and provide reasonable assurance regarding the achievement of entity objectives.*”³

FERMA believes that to be practical within an organisation, the Guidelines should address first these aspects of non-financial information disclosure:

- 1- **Understandability:** the language and the format should be broadly understood by most of the organisation’s workforce;
- 2- **Reliability:** decision-making is increasingly data-driven and the quality of these data is of utmost importance for the credibility of the non-financial statement;
- 3- **Comparability:** it is important to set up the right KPIs and review periodically the efficiency of the organisation response to the identified risks.

Q2 Who should be considered in your opinion the main audience of the non-financial statement?

FERMA believes that each person within the company should receive information about the risks for which they are responsible and able to act on. In order to foster a culture of integrated risk management across the organisation, the non-financial statement should therefore primarily target an internal audience. This document should help all parts of an organisation to work collaboratively on risk management through integrated planning. In January 2016, FERMA supported the call of the World Economic Forum for a culture of integrated risk management to create resilience.⁴ To avoid blind spots that occur by considering different risks in “individual silos”, FERMA promotes the risk management profession coordinating the various risk

³ See Committee of Sponsoring Organizations of the Treadway Commission (COSO), (2004). *Enterprise Risk Management — Integrated Framework Executive Summary* (p. 2). Retrieved from http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf
For similar definitions see also:

RIMS Strategic and Enterprise Risk Center. RIMS the Risk Management Society. Retrieved from <https://www.rims.org/resources/ERM/Pages/WhatIsERM.aspx>

The Institute of Internal Auditors (IIA), (2009). *IIA POSITION PAPER: THE ROLE OF INTERNAL AUDITING IN ENTERPRISE-WIDE RISK MANAGEMENT* (p. 2). Retrieved from <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf>

⁴ FERMA, (2016). *FERMA welcomes Global Risks Report 2016 call for a culture of integrated risk management.* Retrieved from <http://www.ferma.eu/blog/2016/01/ferma-welcomes-global-risks-report-2016-call-culture-integrated-risk-management/>



exposures as a risk portfolio. The objective is to understand the relationships between risks and identify connexions that were not anticipated.

The inability to execute decisions is one of the main reasons why organisations fail. This integrated reporting is expected to provide decision-makers with broader and more structured information. However, to ensure that the organisation is implementing new strategies and targets decided according to these new information, the reporting needs to be first explained internally. The risk manager is responsible for communicating the risk management approach, in an educational way, by explaining the link between risk assessments, mitigation, while ensuring that all relevant players are involved in the process.

Q3 In your opinion, what features make a piece of information material/relevant for the purposes of the non-financial statement?

FERMA is convinced that to set up relevant reporting, the objectives of such exercise must first be known – i.e. who will use the information and for what purpose? The non-financial statement must explicitly mention these objectives.

To establish these objectives, the non-financial statement should refer to a clear and pre-existing vision of the company's general risk management policy and a deep understanding of the business model of the organisation. The risk management process (see Q 5 below) will have identified those risks which have the potential to have an important impact on the business and which, therefore, should be disclosed.

As a consequence, FERMA believes that the criteria to decide if information is material and relevant enough for the non-financial statement is **the potential impairment of the organisation objectives on value and trust** if the undisclosed information is "discovered" by stakeholders (investors, rating agencies, financial analysts, NGOs and regulators).

For FERMA, the role of the risk manager is to define the implementation strategy of this general risk management policy, which is then approved by the risk management committee. At this stage, the management and board of directors of the company know the main areas of risk, which have been identified through a bottom-up approach.



II. Content of the non-binding guidelines

Q5 Please, provide a brief description of how you think that the following matters should be treated in the GUIDELINES, including as appropriate how they should be defined and described?

Principal risks

A risk map should be created. It is a critical component of the risk management process, coordinated by the risk manager who ensures that all the relevant players are involved in the exercise.

Risk mapping allows identification of the areas of risk for each non-financial element and helps to define models for the assessment of the frequency and impact of the risks identified. Risk matrices, which provide a visual understanding of the risks and their relative weights, are here particularly relevant.

Adverse impacts

FERMA strongly recommends the consideration of adverse impacts as the result of an assessment combining both **likelihood and impact levels**.

Risk mitigation measures could be presented according to two main approaches: prevention and protection.

A good understanding of adverse impacts is the starting point to develop control measures and identify potential opportunities.

III. Interaction with other frameworks and other aspects

Q6 How do you think that the GUIDELINES should approach the disclosure of key performance indicators (KPIs)?

FERMA wishes to see the Guidelines to **provide flexibility for organisations to exercise judgement in deciding what KPIs should be included in their disclosures**.

The disclosure of key performance indicators (KPIs) for the monitoring of non-financial elements should be the result of a risk management procedure conducted by the risk manager to identify the organisation's risk profile, followed by an action plan for mitigating risks.

This analysis is produced under a global ERM approach. As mentioned in question 1, comparability of data over time is necessary to set the right KPIs.

It should be noted that some organisations also use some so-called Key Risk Indicators (KRIs) to measure risk trends. Most commonly, however, risk is seen as a KPI moving towards an unwanted direction.



Q8 How do you think that the GUIDELINES should relate to existing national, international or other EU-based frameworks (such as UN Global Compact, the UN Guiding Principles on Business and Human Rights, OECD guidelines for multinational enterprises, the ILO Tripartite Declaration of principles concerning multinational enterprises and social policy, EMAS, etc.)?

In addition to frameworks developed by public entities, the Guidelines should help organisations to report risks on non-financial elements using an ERM approach.

Guidelines should refer to a limited number of frameworks. The criteria for a framework to be mentioned in the Guidelines should be linked to its level of practicality (i.e. how it can be implemented in any business within a decent timeframe) and its acknowledgment by the business community.

In that respect, FERMA recommends that the Guidelines refer to risk management frameworks developed by national risk management associations in Europe such as “The Risk Manager Framework” developed by AMRAE (France) or the “Structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000” developed by AIRMIC (UK) in collaboration with the public sector risk management association (Alarm) and the Institute of Risk Management (IRM).⁵

The process of risk identification, analysis and control, as well as consultation and communication should be conducted preferably in accordance with the ISO 31000 or the COSO ERM Framework, which both are internationally recognised and applied Standards.⁶

⁵ Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE), (2016). *The Risk Manager Framework*. Available online at http://www.amrae.fr/sites/default/files/fichiers_upload/RiskManagerFramework_AMRAE_2013_0.pdf

The Association of Insurance and Risk Managers (AIRMIC), Public Risk Management Association (ALARM), Institute of Risk Management (IRM). (2010). *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000* (online resource). London, England: Authors.
Available online at https://www.theirm.org/media/886062/ISO3100_doc.pdf

See also : Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali (ANRA), (2011). *Risk Management Standards and ISO 31000 - ANRA Position Paper*. Available online at http://www.strategicagroup.com/includes/pdf/Anra_Position_Paper.pdf

⁶ International Standards Organisation (ISO). (2009). *ISO 31000: Risk management – principles and guidelines*.

Available online at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170

Committee of Sponsoring Organizations of the Treadway Commission (COSO),. (2004). *Enterprise Risk Management — Integrated Framework Executive Summary* (p. 2). Retrieved from http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf



Q9 Do you think that when preparing the GUIDELINES only the companies included in the scope of the DIRECTIVE should be considered, or that the interests, characteristics and/or requirements of other companies that prepare management reports should be taken into account as well?

FERMA urges the Commission to write Guidelines that first address the challenges of the reporting requirements for the organisations within the scope of the Directive only.

After periodic review and once the Guidelines have been recognised as facilitating and improving the level of non-financial reporting for these organisations, possible extensions could be considered.

Contact person: Julien Bedhouche, FERMA EU Affairs Adviser, julien.bedhouche@ferma.eu

FERMA - The Federation of European Risk Management Associations brings together 23 national risk management associations in 21 European countries. FERMA represents the interests of over 4700 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