**Michele SIRI** *

# CORPORATE GOVERNANCE OF INSURANCE FIRMS AFTER SOLVENCY II **

*Abstract:* Under Solvency II, corporate governance requirements are a complementary, but nonetheless essential, element to build a sound regulatory framework for insurance undertakings, also to address risks not specifically mitigated by the sole solvency capital requirements. After recalling the provisions of the second pillar concerning the system of governance, the paper is devoted to highlight the emerging regulatory trends in the corporate governance of insurance firms. Among others, it signals the exceptional extension of the duties and responsibilities assigned to the Board of directors, far beyond the traditional role of both monitoring the chief executive officer, and assessing the overall direction and strategy of the business. However, a better risk governance is not necessarily built on narrow rule-based approaches to corporate governance.

*Key words*: Insurance – Corporate Governance - Board of Directors - Culture - Risk Management - Internal Controls – Principle of Proportionality – Regulation – EIOPA – Solvency - Guidelines

*Index:* 1. Introduction. - 2. The system of governance in the Solvency II framework. - 3. General governance requirements. - 4. Fit and proper. - 5. Risk management system. - 6. Toward an 'effective' Board governance. - 7. Role of the Board assuring a 'fair treatment' of customers. - 8. Ratings and quality assessments of corporate governance. - 9. Remuneration. - 10. Final remarks. - References.

## 1. INTRODUCTION

Corporate governance refers to the relationship between a company's senior management, its Board of directors, its shareholders and other stakeholders and determines the structure used to define a company's objectives, as well as the means to achieve them and monitor

---

* University of Genoa – Law Department – E-mail: michele.siri@unige.it

** Forthcoming in "Insurance Regulation in the European Union: Solvency II and Beyond", edited by P. Marano – M. Siri, Palgrave MacMillan, London, 2017. The Author thanks seminar audiences at Catholic University, November 2015, and at International Center for Insurance Regulation, Goethe University, Frankfurt, March 2016, for many useful comments.

the results obtained [1]. Since the 1970s, managerial accountability, Board structure and shareholders' rights have become central issues, especially with regards to listed companies. This new attention to corporate governance issues quickly set up a link among corporations, academia and private practice. While corporate governance has traditionally been recognised as a global movement, industrial companies and financial institutions underwent a different path. Although several regulations have targeted the banking and insurance industry with the goal to enhance corporate governance requirements specific to these sectors and, in particular, to implement efficient internal control systems, the supremacy of the chief executive officer has actually continued to be a dominant feature of the financial sector, also after the financial scandals of the early 2000s[2].

In the financial services sector, corporate governance should take account of the interests of other stakeholders (depositors, savers, life insurance policy holders, etc.), as well as the stability of the financial system, due to the systemic nature of many players [3]. The interests of financial institutions' creditors (depositors, life insurance policy holders, beneficiaries of pension schemes, and, to a certain extent, employees) are potentially at odds with those of their shareholders. The latter benefit from a rise in the share price and maximisation of profits in the short term and are potentially less interested in too low a level of risk. For their part, depositors and other creditors are focused only on the financial institution's ability to repay their deposits and other mature debts, and thus on its long-term viability [4].

Largely as a result of the particularities relating to the nature of their activities, most financial institutions are strictly regulated and supervised. More clearly, the internal governance of financial institutions cannot be reduced to a simple problem of conflicts of interest between shareholders and management. Consequently, according to the European approach, the rules of corporate governance within financial institutions must be adapted to take account of the specific nature of these companies

[1] G20/OECD, *Principles of Corporate Governance*, 2015, p. 9, available at http://www.oecd.org/.

[2] B. CHEFFINS, *The Corporate Governance Movement, Banks and the Financial Crisis*, *Theoretical Inquiries in Law*, vol. 16 n.1, 2015, p.1.

[3] EUROPEAN COMMISSION, *Green Paper, Corporate governance in financial institutions and remuneration policies*, COM (2010), 284 final, p. 3, available at http://ec.europa.eu/internal_market/.

[4] P.O. MULBERT, *Corporate Governance of Banks*, European Business Organisation Law Review, v.11 n.3, 2008, p. 427. See also R.D. CITLAU – P.O. MULBERT, *The uncertain role of banks' corporate governance in systemic risk regulation*, ECGI Law Working Paper n. 179, 2011, available at www.ecgi.org/wp.

[5]. As to the insurance sector, it is worth noting that in both the US and Europe a new regulatory intervention was supported, albeit with different goals. In fact, in the US the supervision of the insurance industry – in order to improve the state-based regulatory system for financial stability – seems to have been the main concern of post-crisis reforms. In Europe, prudential supervision has been a major concern, although the Solvency II directive deals not only with capital requirements, but also with governance issues.

The 2008 financial crisis showed that financial institutions' corporate governance was unsuccessful mainly because of the excessive risk-taking, boosted by generous executive remuneration [6]. In this scenario, the insurance industry has been less affected by the financial crisis in comparison to the banking system, although it was still partially involved in the derivatives turbulence (e.g., AIG in the United States) [7]. Consequently, various reforms relating to banks, insurance and investment firms have been enacted in response to the financial crisis. However, the US and Europe have not followed an identical approach. The main focus of the Dodd Frank Act lies on financial stability, disclosure and transparency requirements, rather than on corporate governance, with the exception of "say on pay", proxy access and disclosure on the separation of the roles of chief executive officer and chairman. By contrast, the European Union has seemingly reserved more attention to corporate governance issues [8]. Special consideration has been

---

[5] EUROPEAN COMMISSION, *Green Paper, Corporate governance in financial institutions and remuneration policies*, COM (2010), 284 final, p. 4. For a critical view on stakeholder governance see G. FERRARINI, *Understanding the Role of Corporate Governance in Financial Institutions: A Research Agenda*, Law Working Paper n. 347, 2017, available at www.ecgi.org/wp.

[6] DE LAROSIÈRE HIGH LEVEL GROUP, *Report on the future of financial supervision in the EU*, 25 February 2009, Brussels. The Report stated that corporate governance was one of the most important elements underlying the financial crisis. Corporate governance failure was not the only cause of the financial crisis and probably not even the most important one. Other factors played a crucial role, such as "the lax monetary policy of the American Federal Reserve Bank, the policy and practice of credit financing the housing of broad masses of the population, the securitisation of credit in complicated and opaque financial instruments": see K. HOPT, *Corporate Governance of Banks and Other Financial Institutions after the Financial Crisis*, J. Corp. L. Studies, 2013, p. 237.

[7] In the aftermath of the crisis, US regulators and scholars question the effectiveness of the existing corporate governance system in overseeing insurance companies and their excessive risk taking; see N. BOUBAKRI, *Corporate governance and issues from the insurance industry*, Journal of Risk and Insurance, 78, 2011, 3, p. 501.

[8] In the banking sector with the CRD IV Directive 2013/36/UE and the Regulation n.575/2013 on prudential requirements for credit institutions and investments firms (the so-called CRD IV/CRR regime) the European legislator has introduced a comprehensive governance framework for banks. In the securities sector the MiFID II Directive 2014/55/EU and the Regulation 600/2014 (the so-called MiFID framework) include key governance requirements of the CRD IV Directive relating to, in particular, the

given to the structure and functioning of the Board, the risk management policy and internal control system, and the executive remuneration and supervision [9]; still, at the core of the European reforms in reaction to the perceived governance failure stands the idea of strengthening the role of the Board to avoid excessive and imprudent risk-taking [10].

As for the corporate governance of banks, even if similar conclusions can be assumed to hold for the entire financial institution, scholars have argued that the primary justification for regulating internal control systems is to maximise the "efficiency" with which exposure to risk is managed [11]. It is a very different focus, far from the traditional approach to governance with emphasis on shareholder rights [12]. Moreover, the banks with the most 'pro-shareholder' Boards and the closest alignment between executive returns and stock price were those which took the most risks prior to, and suffered the greatest losses during, the crisis. Consequently, a significant rethink about the way in which banks are governed is required [13]. Therefore, one of the primary objectives of international standard setters in the banking sector is to provide guidance for supervisors that favours "weaker rights" for

---

composition and the obligations of the Boards into the legal regime applicable to the investment firms. See N. MOLONEY, *EU Securities and Financial Markets Regulation*, 2014, p. 357 ff.

[9] M. HILB, *Redesigning corporate governance: lessons learnt from the global financial crisis*, Journal of Management and Governance, v. 15 n.4, 2011, p. 533 ff. See also OECD STEERING COMMITTEE ON CORPORATE GOVERNANCE, *Corporate governance and the financial crisis*, p. 15, available at http://www.oecd.org/.

[10] J. WINTER, *The Financial Crisis: Does Good Corporate Governance Matter and How to Achieve it?* in E. Wymeersch, K.J. Hopt, and G. Ferrarini (eds.), *Financial Regulation and Supervision. A post-crisis analysis*, 2012, para. 12.

[11] L. PI - S.G. TIMME, *Corporate control and bank efficiency*, Journal of Bank and Finance, vol. 17 n.2-3, 1993, p. 515; R. LEVINE, *The corporate governance of banks: a concise discussion of concepts and evidence*, World Bank Policy Research Working Paper, n. 3404, 2004, available at http://documents.worldbank.org/; G. KIRKPATRICK, *The corporate governance lessons from the financial crisis*, Financial Market Trends, 2009, 3(1), available at http://search.oecd.org/finance/financial-markets/. See also for the insurance sector see P. MANES, *Corporate Governance, the Approach to Risk and the Insurance Industry under Solvency II*, in M. Andenas – R.G. Avesani – P. Manes – F. Vella – P.R. Wood (eds.), *Solvency II: A Dynamic Challenge for the Insurance Market*, Il Mulino, 2017, chapter IV, p. 93 ff., and O. RICCI, *Corporate Governance in the European Insurance Industry*, Springer, 2014.

[12] Banks with the most shareholder-friendly governance performed worst during the crisis of 2007– 2008 as demonstrated by A. BELTRATTI – R.M. STULZ, *Why did some banks perform better during the credit crisis? A cross-country study of the impact of governance and regulation*, Journal of Financial Economics 105, 2012, p. 1.

[13] J. ARMOUR – D. AWREY – P.L. DAVIES – L. ENRIQUES – J.N. GORDON – C. MAYER – J. PAYNE, *Bank Governance*, ECGI Working Paper N°. 316/2016, June 2016, available at www.ecgi.org/wp.

shareholders and "stronger rights" for other stakeholder groups [14]. This is commonly referred to as "risk governance", because the focus is on ensuring that risks are adequately managed and disclosed [15].

The effectiveness of the corporate governance of financial institutions is thus a central topic of international standard setters in the banking sector [16] and has been included into the regulatory framework of the guidelines and technical advices issued by the European Supervisory Authorities for the all financial institutions [17]. Recent significant risk incidents and corporate scandals caused by misconduct in the banking sector suggest that financial institutions need to further enhance corporate governance measures as well ethics and culture [18]. The European legislation after the financial crisis clearly shows that the regulation of corporate governance goes beyond the traditional approach of company law, because the governance regime shall ensure not only the "integrity of the market" [19] to reduce the excessive risk-taking, but also the "investor protection" as far as the MiFID regime is concerned.

---

[14] BASEL COMMITTEE ON BANKING SUPERVISION, *Principles for enhancing corporate governance*, 2010, available at www.bis.org. See at par. 13: "Indeed, in addition to their responsibilities to shareholders, banks also have a responsibility to their depositors and to other recognised stakeholders. The legal and regulatory system in a country determines the formal responsibilities a bank has to its shareholders, depositors and other relevant stakeholders. This document will use the phrase "shareholders, depositors and other relevant stakeholders," while recognising that banks' responsibilities in this regard vary across jurisdictions.".

[15] FINANCIAL STABILITY BOARD, *Thematic review on risk governance*, 2013, available at www.financialstabilityboard.org.

[16] S. WRIGHT – E. SHEEDY – S. MAGEE, *International compliance with new Basel Accord principles for risk governance*, Account. Finance, 2016, available at https://doi:10.1111/acfi.12213.

[17] ESA 3L3 TASK FORCE ON INTERNAL GOVERNANCE, *Cross-sectoral stock-take and analysis of internal governance requirements*, October 2009, available at https://www.eba.europa.eu. For the last developments in the banking and securities sectors see: EBA, *Draft Guidelines on internal governance*, Consultation Paper, 28.10.2016, available at https://www.eba.europa.eu; ESMA – EBA, *Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU*, Consultation Paper, 28.10.2016, available at https://www.esma.europa.eu/.

[18] GROUP OF THIRTY, *Banking conduct and culture: a call for sustained and comprehensive reform*, July 2015, available at http://group30.org; FINANCIAL STABILITY BOARD, *Guidance on supervisory interaction with financial institutions on risk culture*, April 2014, available at http://www.fsb.org/; EUROPEAN SYSTEMIC RISK BOARD, *Report on misconduct risk in the banking sector*, June 2015, available at https://www.esrb.europa.eu/.

[19] See MiFID II Directive, Recital 53: "It is necessary to strengthen the role of management bodies of investment firms, regulated markets and data reporting services providers in ensuring sound and prudent management of the firms, the promotion of the integrity of the market and the interest of investors.". See C. E. DE JAGER, *A Question*

The focus on public trust is even more apparent in insurance legislation. In fact, the main goal of the Solvency II directive is to ensure an adequate protection of policyholders and beneficiaries, also through a new risk management, financial reporting and corporate governance assessment [20]. Unlike banking regulation, financial stability and fair and stable markets, albeit important objectives of the insurance and reinsurance regulation, should not impair the main objective [21]. Therefore, in the insurance sector the regulation and supervision of the internal governance mechanisms is an essential part of the framework of risk management, because some risks may only be properly addressed through governance requirements. An effective system of governance requires a proactive approach on the part of insurance firms, with a significant impact on the duties and obligations of the members of the Board, on the one hand, and on the supervisor's ability to assess the compliance of the internal governance with these specific requirements, on the other [22].

Last but not least, ineffective internal control systems in banking institutions have also been significant factors in several incidents of fraud [23]. This has called for closer cooperation between regulators, and external and internal auditors, so as to win back public trust in financial

*of Trust: the Pursuit of Consumer Trust in the Financial Sector by Means of EU Legislation*, J. Consumer Policy, 40, 2017, p. 25, at p. 24.

[20] M. DREHER, *Treatise on Solvency II*, Springer, 2015. The Author clearly states, at chapter 3 p. 67 ff., that consumer Protection is not addressed in Solvency II directive as well as in the Level 2 and 3, being the protection of policy holders and beneficiaries of indemnity payments the main objective of Solvency II. Therefore, "consumer protection is a significant by-product of the Solvency II rules", and the "EIOPA provisions, too, address consumer protection solely in the realm of collective consumer protection".

[21] See Solvency II Directive, Recital 16: "The main objective of insurance and reinsurance regulation and supervision is the adequate protection of policy holders and beneficiaries. The term beneficiary is intended to cover any natural or legal person who is entitled to a right under an insurance contract. Financial stability and fair and stable markets are other objectives of insurance and reinsurance regulation and supervision which should also be taken into account but should not undermine the main objective.".

[22] See Solvency II Directive, Recital 29: "Some risks may only be properly addressed through governance requirements rather than through the quantitative requirements reflected in the Solvency Capital Requirement. An effective system of governance is therefore essential for the adequate management of the insurance undertaking and for the regulatory system.".

[23] W. ERHARD – M. JENSEN, *Putting integrity into finance: a purely positive approach*, ECGI Finance Working Paper, last rev. 2015, 417, Appendix 1, available at http://www.ecgi.org.

institutions [24]. It is worth noting that, also in the insurance market, before the financial crisis, the report by Sharma [25] identified a causal relationship between firms that either fail or are inherently vulnerable and 'underlying management weakness or operational weakness'. Good governance practices and strong risk management are therefore essential aspects of a prudential regulatory framework [26].

## 2. THE SYSTEM OF GOVERNANCE IN THE SOLVENCY II FRAMEWORK

The Solvency II requirements are designed to provide an enhanced and more consistent level of protection for policyholders throughout Europe and are structured into three 'pillars' that cover quantitative requirements, qualitative requirements and supervisory review, and reporting and disclosure [27]. Solvency II seeks to ensure that firms identify, quantify and manage their risks on a proportionate and forward-looking basis. In this regard, it introduces improved governance and risk management requirements. It is worth saying that Solvency II is a largely 'maximum harmonising' regulatory framework, which

---

[24] I. ARNDORFER – A. MINTO, *The "four lines of defence model" for financial institutions*, BIS Financial Stability Institute, Occasional Paper n. 11, 2015, p. 3, available at http://www.bis.org/fsi/.

[25] CONFERENCE OF INSURANCE SUPERVISORY SERVICES OF THE MEMBER STATES OF THE EUROPEAN UNION, *Prudential supervision of insurance undertakings*, Report prepared under chairmanship of Paul Sharma, 2002, available at http://ec.europa.eu/internal_market/insurance/. This "Sharma Report" highlighted that the supervisory regime should focus not only on the financial resilience of insurance undertakings but also on their governance and risk management systems (see Sharma p. 70 ff.). This approach is reflected in the Solvency II Directive, which states that "Some risks may only be properly addressed through governance requirements rather than through the quantitative requirements .... An effective system of governance is therefore essential for the adequate management of the insurance undertaking and for the regulatory system.".

[26] R. SWAIN – D. SWALLOW, *The prudential regulation of insurers under Solvency II*, Bank of England, Quarterly Bulletin 2015 Q2, p. 145, available at http://www.bankofengland.co.uk/.

[27] The initial work for the EC Solvency II project was largely based on the Basel II framework for banking regulation and the three pillars approach have been discussed in a report commissioned by the Internal Market Directorate General of the European Commission: KPMG, *Study into the methodologies to assess the overall financial position of an insurance undertaking from the perspective of prudential supervision*, May 2002, available at http://ec.europa.eu/internal_market/insurance/. See also J. VAN DER ENDE – R. AYADI, *Insurance Regulation and Supervision in the EU: Report of a CEPS Task Force*, Brussels, 2006 and A.V. GUCCIONE, *From Solvency to Omnibus. Historical Origins and Normative Evolution*, in M. Andenas – R.G. Avesani – P. Manes – F. Vella – P.R. Wood (eds.), *Solvency II: A Dynamic Challenge for the Insurance Market*, Il Mulino, 2017, chapter I, p. 35 ff.

introduces a single set of requirements that are to be applied consistently across Europe. The Directive already comprises a considerably high level of detail concerning principles and requirements of the system of governance, especially compared to the Level 1 and/or Level 2 texts implementing measures of other EU directives on financial services.

The Solvency II directive covers the most important issues to be regulated to ensure appropriate governance standards within insurance and reinsurance undertakings. Therefore, the scope of essential and extensive measures on Level 2 has been limited [28]. Moreover, article 50 of the Directive stipulates the minimum contents of the Level 2 implementing measures. These are the reasons why the provisions of the second pillar concerning the corporate governance of insurance undertakings shall also include the EIOPA Guidelines supplementing the Solvency II requirements, as provided by the Directive and the Implementing Measures, to foster supervisory convergence.

With regards to the overall system of governance for insurance and reinsurance undertakings, Section 2 of Chapter IV of the Solvency II directive focuses on the regulation of the following main issues: general governance requirements, fit and proper requirements, risk management, internal control, outsourcing, and the prudent person principle. The "general governance requirements" (art. 41) aims at the implementation of an effective and proportionate system of governance, which provides for sound and prudent management of the business and sets out the implementation of written policies concerning the main functions of the undertaking (i.e. risk management, internal audit,

[28] CEIOPS, *Advice for Level 2 Implementing Measures on Solvency II: System of Governance* (former Consultation Paper 33), October 2009, p. 3, available at https://eiopa.europa.eu/CEIOPS-Archive/. The Advice, at para. 1.3, remarks that "the Level 1 text already comprises a considerably high level of detail concerning principles and requirements on the system of governance, especially compared to the Level 1 text and/or Level 2 implementing measures in other EU directives on financial services." Accordingly, there is any general Level 2 provision in the implementing measures with regard to proportionality. No doubt that proportionality requirement applies to every element of the system of governance. However, it is the responsibility of the administrative, management or supervisory body to ensure that the undertaking's organisational structure delivers a system of governance proportionate to the nature, scale and complexity of the risks it faces in its business activities. Regarding the fulfilment of the internal audit function it should be noted that this cannot be combined with other operational duties or functions. the internal audit function shall be objective and independent from the operational functions. In effect, this means that in the view of the Solvency II regime, the internal audit function – in contrast to the other functions explicitly mentioned in the Directive – needs to be a separate unit or an individual without other duties within the undertaking, unless the function is outsourced. See CEIOPS, *Advice to the European Commission on the Principle of Proportionality in the Solvency II Framework Directive proposal*, CEIOPS-DOC-24/08, May 2008, available at https://eiopa.europa.eu/CEIOPS-Archive/.

internal control, outsourcing), including the development of contingent plans. The “fit and proper requirements for persons who effectively run the undertaking or have other key functions” (art. 42-43) aims to ensure that all the persons that effectively manage the undertaking or perform key functions within the undertaking are fit and proper, meaning that they comply with both professional and reputational standards. The “risk management” (art. 44) aims at the implementation of an effective risk management system within the undertaking, comprising strategies, processes and reporting procedures necessary to identify and manage the main risks to which the undertaking is exposed, at both an individual and group level, including the “own risk and solvency assessment” activity (art. 45). “Internal control”, “internal audit” and “actuarial function” (art. 46-48) aim at ensuring the implementation of effective internal control system, internal audit function and actuarial function with the undertaking.

These governance requirements are addressed and, in some cases, further developed in the Implementing Measures and the EIOPA Guidelines on the System of Governance. It is worth remembering that both the Solvency II directive and the EIOPA Guidelines are addressed to the competent national authorities that should implement – at the national level – suitable measures within the specified time framework to ensure compliance with the provisions of the Solvency II directive and the EIOPA Guidelines [29]. This paper analyses the EIOPA Guidelines, with a special focus on what we consider to be the most relevant provisions to achieve a suitable governance.

## 3. GENERAL GOVERNANCE REQUIREMENTS

The Directive requires all insurance and reinsurance undertakings to have in place an effective system of governance which provides for the sound and prudent management of the business [30]. That system shall at least include an adequate transparent organisational structure with a

[29] EIOPA, *Guidelines on system of governance*, 28 January 2015, EIOPA-BoS-14/253, available at https://eiopa.europa.eu/. The “General Governance requirements” are detailed in Section 1 (Guidelines 1-8), “Remuneration” in Section 2 (Guideline 9-10), “the Fit and Proper” in Section 3 (Guidelines 11 to 16), the “Risk Management” in Section 4 (Guidelines 17-26), the “Prudent person principle” in Section 5 (Guidelines 27-35).

[30] P. MANES, *Corporate Governance, the Approach to Risk and the Insurance Industry under Solvency II*, in M. Andenas – R.G. Avesani – P. Manes – F. Vella – P.R. Wood (eds.), *Solvency II: A Dynamic Challenge for the Insurance Market*, Il Mulino, 2017, chapter IV, p. 115 ff.,

clear allocation and appropriate segregation of responsibilities, as well as an effective system for ensuring the transmission of information [31].

In line with corporate governance best practices, the EIOPA Guidelines put particular emphasis on the company's organization referring, as usual, to four main areas: an effective system of governance (comprising risk), the internal control system, the organisational and operational structure and the decision-making process. Therefore, in an enlarged perspective, most EIOPA Guidelines do not present a particular degree of innovation, except for some aspects that are nonetheless open to debate. Like with the existing governance requirements for credit institutions and investment firms set out in the regimes laid down in the Capital Requirements Directive and the Markets in Financial Instruments Directive, also under Solvency II Directive the administrative, management or supervisory body [32] is at the centre of the governance system.

---

[31] According to the Implementing Measures (art. 258) the undertaking's system of governance should: (a) establish, implement and maintain effective cooperation, internal reporting and communication of information at all relevant levels of the undertaking; (b) establish, implement and maintain effective decision making procedures and an organizational structure which clearly specifies reporting lines, allocates functions and responsibilities, and takes into account the nature, scale and complexity of the risks inherent in that undertaking's business; (c) ensure that the members of the administrative, management or supervisory body collectively possess the necessary qualifications, competency, skills and professional experience in the relevant areas of the business in order to effectively manage and oversee the undertaking in a professional manner; (d) ensure that each individual member of the administrative, management or supervisory body has the necessary qualifications, competency, skills and professional experience to perform the tasks assigned; (e) employ personnel with the skills, knowledge and expertise necessary to carry out the responsibilities allocated to them properly; (f) ensure that all personnel are aware of the procedures for the proper carrying out of their responsibilities; (g) ensure that the assignment of multiple tasks to individuals and organisational units does not or is not likely to prevent the persons concerned from carrying out any particular function in a sound, honest and objective manner; (h) establish information systems which produce complete, reliable, clear, consistent, timely and relevant information concerning the business activities, the commitments assumed and the risks to which the undertaking is exposed; (i) maintain adequate and orderly records of the undertaking's business and internal organisation; (j) safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question; (k) introduce clear reporting lines that ensure the prompt transfer of information to all persons who need it in a way that enables them to recognize its importance as regards their respective responsibilities; (l) adopt a written remuneration policy.

[32] The nature and structure of the administrative, management or supervisory body varies with the national company law applicable in the jurisdiction in which the insurance undertaking is incorporated. The term "administrative, management or supervisory body" covers the single Board in a one-tier system and the management or the supervisory Board of a two-tier Board system. According to the Directive, the responsibilities and duties of the different bodies should be seen having regard to different national laws.

The first Guideline of the general governance requirements (Guideline 1) focuses on the duty of the administrative body to be informed [33]. Committees (if established), senior management and key functions are the interlocutors with whom the Board has to interact, "proactively requesting information from them and challenging that information, when necessary". It seems not possible to overlook that the provision requires directors to behave proactively. This means that the Board has to carry out a rather strict duty of monitoring. Indeed, directors not only have to check the information provided, but should also collect sensible information on their own. This solution could affect the general principle that directors can rely on officers' information. In this case, the liability area of non-executive directors would increase dramatically. Furthermore, it is necessary to highlight that the Solvency II directive does not make any explicit reference to a proactive behaviour, but it rather refers to, among others, an effective system of governance and requires to set up an appropriate segregation of responsibilities. It is questionable whether a too wide monitoring duty fits with effectiveness, and whether it allows to easily separate executive and non-executive tasks.

Moving to the organisational and operational structure (Guideline 2), a close link exists between organization and effective operation, provided that they support each other. Both are necessary to ensure a proper flow of information among the undertaking's different levels of hierarchy. In this regard, the organization structure determines the tasks and assignments, while the operational structure settles the way of performing the tasks. In any case, it is ultimately the administrative,

---

When transposing the Level 1 text, each Member State has to consider its own system and attribute each responsibility and duty to the appropriate Board.

[33] According to CEIOPS, the predecessor of EIOPA, the administrative, management or supervisory body is ultimately accountable and responsible for the compliance of the undertaking with legal and administrative requirements pursuant to the Directive. Therefore, "[d]elegating to committees consisting of members of the administrative, management or supervisory body does not in any way release the administrative, management or supervisory body from collectively discharging its duties and responsibilities. The administrative, management or supervisory body needs to ensure that it has regular and robust interaction with any Board committee on the one hand, and with senior management and with key functions on the other hand, and to recognise that part of its duties include requesting information proactively and challenging this information when necessary" (CEIOPS, *Advice for Level 2 Implementing Measures on Solvency II: System of Governance*, October 2009, p. 10, para 3.4, available at https://eiopa.europa.eu/CEIOPS-Archive/. Therefore, each undertaking's administrative, management or supervisory body should consider whether the structure of a committee is appropriate (e.g. forming audit, risk, investment or remuneration committees) and, if so, what its mandate and reporting lines should be. See also K. VAN HULLE, *The challenge of Solvency II: Lecture to the faculty of actuaries*, British Actuarial Journal, 2008, 14, 1, p. 27.

management or supervisory body (AMSB) that has the responsibility of execution and is not bound by the suggestions in the findings of the key functions. Although the EIOPA clearly states in the explanatory text to Guideline 5 that the AMSB is obviously not entitled to suppress or tone down the results of the key functions [34], it is not clear how the AMSB can reach different conclusions without pressing the several functions in order to get new data able to support its position. A similar problem raises in relation to the Guideline 4, which requires the undertaking to appropriately document the decisions taken at the AMSB level. Moreover, this provision determines how the information flow from the risk management system has to be taken into account. If the first part of this provision is clearly aiming to make the decisions of the AMSB traceable, the second part is quite ambiguous, in that it does not specify in which way and under which conditions the AMSB can move away from the results of risk management.

Lastly, organisation and operation structure are based on a cost and benefit approach. This represents a fundamental change to the Solvency I directive, that was based on the 'one size fits all' principle. This new approach, on the one side, introduces more flexibility in corporate governance system of each undertaking and, on the other side, increases the responsibility of the Board, when compared to the previous regulatory framework. Obviously, undertakings have to review their system of governance periodically (and in the case of particularly significant events), under the ultimate responsibility of the ASMB (Guideline 6) [35]. In relation to key functions, the EIOPA does not requires mandatory organisational structure of separate units focusing on risk management, compliance, internal audit and actuarial function [36]. Still, the

[34] EIOPA, *Final Report on Public Consultation No. 14/017 on Guidelines on system of governance*, available at https://eiopa.europa.eu/, at part 2, n. 2.17, states: "The AMSB does not exert influence to suppress or tone down key function results in order that there is no discrepancy between the findings of key functions and the AMSB's actions.".

[35] Undertakings have to ensure that the system of governance is internally reviewed on a regular basis. To this purpose, according to para n. 3.13-3.14 of the Advice, they have to determine the appropriate frequency of the reviews taking into account the nature, scale and complexity of their business and assign responsibility for the review. be documented as appropriate. Suitable feedback loops should exist to ensure follow-up actions are continuously undertaken and recorded. In order to allow an adequate revision of the system of governance, appropriate reporting procedures encompassing at least all key functions should be established. The reports to be produced shall encompass an assessment of the effectiveness of the system of governance and should contain suggestions for improvements. They should be presented to the administrative, management or supervisory body at least annually, according to the principle of proportionality, and discussions on any challenge provided or improvements suggested should be documented as appropriate. Suitable feedback loops should exist to ensure follow-up actions are continuously undertaken and recorded.

[36] According to the para. 3.11 of CEIOPS Advice "The undertaking should ensure that each key function has an appropriate standing in terms of organisational structure.

undertaking may combine each function based on its own features. Moreover, the Solvency II regime provides a mandatory model for the written policies required by Art. 41, sec. 3, Solvency II (risk management, internal control, internal audit and, where relevant, outsourcing) and for any further policy the undertaking decides to implement (Guideline 9).

It is uncertain whether it is possible to infer from the Directive (Chapter IV, Section 2) that the "four-eyes principle" (i.e., the principle that, prior to "implementing" any significant decision concerning the undertaking, at least two persons must review any such decision) should be complied with by all (re)insurance undertakings. Supporting the view of the CEIOPS, the Implementing Measures states that, in line with the existing requirements for other financial sectors, in the context of the system of governance, insurance and reinsurance undertakings "shall ensure that at least two persons effectively run the undertaking" (art. 258 par. 4) [37]. The EIOPA includes some more specific requirements with reference to the four-eyes principle. As for the decision-making process, according to the EIOPA, the four-eyes principle foresees that every significant decision is effectively taken by at least two persons "before the decision is being implemented" (Guideline 3). Significant decisions are decisions that are unusual or that could have a material impact on the undertaking (Guideline 3) [38].

The Guideline does not specify whether these two persons must necessarily be directors or not. Arguably, the second option is the most sensitive, because the provision refers generally to "persons". Several

---

Considering the principle of proportionality, CEIOPS believes that in large undertakings and in undertakings with more complex risk profiles the key functions should generally be performed by separate units" (CEIOPS, *Advice for Level 2 Implementing Measures on Solvency II: System of Governance* (former Consultation Paper 33), October 2009, p. 12, para 3.10, available at https://eiopa.europa.eu/CEIOPS-Archive/. An adequate interaction between the key functions has to be fostered and adequately defined by each undertaking, including the establishment of communication and reporting procedures. In this context, all key functions should have access rights to the relevant systems and staff members, including any records, necessary to allow them to carry out their responsibilities.

[37] CEIOPS, *Advice for Level 2 Implementing Measures on Solvency II: System of Governance* (former Consultation Paper 33), October 2009, p. 12, para 3.3, available at https://eiopa.europa.eu/CEIOPS-Archive/.

[38] EIOPA, *Final Report on Public Consultation No. 14/017 on Guidelines on system of governance*, available at https://eiopa.europa.eu/, at part 2, n. 2.10 states: "Significant decisions as opposed to day-to-day decisions do not concern the spate of usual decisions to be taken at the top level of the undertaking in the running of the business, but are rather decisions that are unusual or that will or could have a material impact on the undertaking. This could be e.g. decisions that affect the strategy of the undertaking, its business activities or its business conduct, that could have serious legal or regulatory consequences, that could have major financial effects or major implications for staff or policyholders or that could potentially result in repercussions for the undertaking's reputation.".

situations could arise in practice, considering, for example, the case of two executive directors or (only) one executive director. In the first hypothesis, if the two executives are in charge of the business and take the decision jointly, there seems to be compliance with the Guidelines. By contrast, the case in which a delegation of different exclusive tasks is given to each director appears to be more problematic [39]. Overall, it seems that in both cases, the question is whether the "two people rule" is aimed to ensure either a better level of competence or a better monitoring function. Considering that quite rarely an undertaking appoints two executives for the same area of competence and that the regulator is well aware thereof, it can be assumed that the goal of this principle is to ensure a better monitoring function.

## 4. FIT AND PROPER

Insurance and reinsurance undertakings shall ensure that all persons who effectively run the undertaking or have other key functions at all times fulfil the following requirements: (a) their professional qualifications, knowledge and experience are adequate to enable sound and prudent management (fit); and (b) they are of good repute and integrity (proper)[40]. These requirements apply to all persons who

---

[39] This situation might not comply with the EIOPA Guidelines, since each director has a different specific area of business. Possible solutions could be to involve the Board or to require the approval of the other executive although in charge of a different area of business. However, in both cases, it is difficult to understand if these solutions comply with the EIOPA Guideline, considering that there is not a definition of the "two people running the business" requirement. On the one hand, it might mean that the executives have to jointly undergo the decision-making process; therefore, neither of the abovementioned solutions would comply with the EIOPA Guideline. On the other hand, though, we could assume that the concept of "effectively running the business" just requires that the people involved in the significant decision manage the undertaking, regardless of their specific area of competences. In the first scenario, there seems to be compliance with the EIOPA Guideline; in the second, it is clear that there is not compliance with the EIOPA Guideline, since only one director has been appointed as executive. As above, a possible solution could be to involve the Board, but the same problems would arise. Other solutions could be the involvement of a non-executive director or of the director general. In the first case, it is difficult to assess that a non-executive director effectively runs the company; in the second, the major concern is the fact that the director general is hierarchically subordinated to the executive director.

[40] See Solvency II Directive at article 42. The Implementing Measures does not specify any general criteria for the assessment of the fitness and propriety – to be developed under the EIOPA Guidelines. Notwithstanding the cross sectoral work in this area of the ESA, the Level 2 should have considered the scope of the assessment of the competence in terms of management and in the area of the business activities carried out by the insurance undertaking. Also, the Implementing Measures, given the absence of any provision in the Directive, contain no rules on the methodology to be followed by supervisory authorities when assessing the suitability of a person, with particular

effectively run the undertaking. The "fit ad proper" requirements are not limited to the members of the AMSB, but could include other persons such as senior managers. Therefore, senior management could include persons employed by the undertaking who are responsible for high-level decision-making, and implementing the strategies devised and the policies approved by the AMSB [41]. The other "key functions" are those considered critical or important in the system of governance, and include at least the risk management, the compliance, the internal audit and the actuarial functions [42]. Other functions may be considered key functions according to the nature, scale and complexity of an undertaking's business or the way it is organised. The fit and proper requirements do apply also in case of outsourcing of key functions to the persons employed by the service provider. The Directive also requires undertakings to notify the supervisory authority whenever the identity of persons running the undertaking or holding other key functions changes [43].

The EIOPA Guidelines clearly reaffirm that the persons that effectively run the undertaking or are in charge of other key functions are fit and that the directors' duties are assigned according to their specific qualifications, knowledge and experience (Guidelines 11-13). With particular regard to the ASMB, this body must collectively possess at least a qualification, experience and knowledge in the following fields: insurance and financial markets; business strategy and business model; system of governance; financial and actuarial analysis; and regulatory framework and requirements. Moreover, the notion of "fitness" provides a partial solution to our previous question about the rationale of the "two persons" rule, since it points out that the members of the AMSB must not have an individual "knowledge, competence and experience" within all

reference to past behaviour, nor provide any clarification of the power to require the undertaking not to appoint, or replace, the person in question.

[41] The Board and the senior management are under strict fit and proper requirements, because they represent the "starting point for setting the undertaking's core values and expectations for the risk culture of the institution": see P. MANES, *Corporate Governance, the Approach to Risk and the Insurance Industry under Solvency II*, in M. Andenas – R.G. Avesani – P. Manes – F. Vella – P.R. Wood (eds.), *Solvency II: A Dynamic Challenge for the Insurance Market*, Il Mulino, 2017, chapter IV, p. 118.

[42] See also M. DREHER, *Treatise on Solvency II*, Springer, 2015, at chapter 7, p. 217 ff., explaining the interplay between the key functions" considered critical or important in the system of governance.

[43] The scope of the information requirement to enable the supervisory authority to assess the fitness and propriety of the persons, is the same as the scope of the notification requirement. It comprises the persons who effectively run the undertaking or those considered critical or important in the system of governance (such as the risk management, the compliance, the internal audit and the actuarial functions), and may in addition include persons responsible for other key functions, depending on the nature, scale and complexity of the business.

areas of the undertakings, but only a “collective” knowledge, competence and experience as a whole, to provide for a sound and prudent management of the firm. Therefore, it seems that the rule that requires two people to effectively run the business wants to ensure a “better monitoring” activity, and the absence in the Level 2 text of a requirement that the members of the AMSB should, as a whole, be able to provide for the “sound and prudent management” of the undertaking is rather regrettable.

In line with article 273 par. 4 of the Implementing Measures, the “proper” requirement refers to the person’s honesty and financial soundness, and is based on the relevant evidence concerning their character, behaviour and business conduct, including any criminal, financial and supervisory aspects, and, obviously, any possible conflicts of interest. Proper considerations are relevant for every person working in the undertaking, although a specific assessment can be applied only to employees. Otherwise, the persons who effectively run the undertaking or have other key functions are always required to have the same adequate level, irrespective of the nature, scale and complexity of the risk of the business or the undertakings’ risk profile [44].

## 5. RISK MANAGEMENT SYSTEM

Insurance and reinsurance institutions shall have in place an effective risk-management system, comprising strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report, on a continuous basis, the risks, at both an individual and aggregated level, to which they are or could be exposed, and their interdependencies [45]. The AMSB is responsible for ensuring that the

[44] It is worth noting that, in relation to the propriety requirement, all persons who effectively run the undertaking or have other key functions should each be proper. According to the CEIOPS Advice, “[t]he proportionality principle does not result in different standards in the case of the propriety requirement, since the repute and integrity of the persons who effectively run the undertaking or hold key functions should always be on the same adequate level irrespective of the nature, scale and complexity of the business or of the undertaking’s risk profile.” (CEIOPS, *Advice for Level 2 Implementing Measures on Solvency II: System of Governance*, October 2009, p. 12, para 3.43, available at https://eiopa.europa.eu/CEIOPS-Archive/).

[45] See Solvency II Directive at article 44. The Implementing Measures requires, at article 259 par. 1, that a risk management system includes: “(a) a clearly defined risk management strategy which is consistent with the undertaking’s overall business strategy. The objectives and key principles of the strategy, the approved risk tolerance limits and the assignment of responsibilities across all the activities of the undertaking shall be documented; (b) a clearly defined procedure on the decision-making process; (c) written policies which effectively ensure the definition and categorisation of the material risks by type to which the undertaking is exposed, and the approved risk tolerance limits for each type of risk. Such policies shall implement the undertaking’s risk strategy,

implemented risk management system is suitable, effective and proportionate to the nature, scale and complexity of the risks inherent in the business, as well as for the approval of any periodic revision of the main strategies and business policies of the undertaking in terms of risk management [46]. Accordingly, the EIOPA Guidelines reflect a common view about the need of the involvement of the Board in the most important corporate issues, clearly including risk management [47].

The Board is the ultimate body responsible for ensuring the effectiveness of the risk management system, setting the undertaking's risk appetite and overall risk tolerance limits, as well as approving the main risk management strategies and policies. In this regard, executive and non-executive directors share the same task; however, given the presence of asymmetric information, they must still be viewed as two different categories (and therefore subject to different liability criteria). It is worth mentioning that the EIOPA affirms that the undertaking is expected to "designate at least one member of the AMSB to oversee the risk management system" on behalf of the Board [48]. This provision is quite ambiguous, because control functions are usually appointed by the top management (provided that they are independent from the executive directors). Therefore, it is rather surprising that the explanatory note assigns this function to a director.

---

facilitate control mechanisms and take into account the nature, scope and time periods of the business and the associated risks; (d) reporting procedures and processes which ensure that information on the material risks faced by the undertaking and the effectiveness of the risk management system are actively monitored and analysed and that appropriate modifications to the system are made where necessary.".

[46] The "strategies" are high-level plans that are developed by the administrative, management or supervisory body and are further specified via policies and business plans to ensure implementation in day-to-day business. The "policies" are internal guidelines established by senior management in line with the relevant strategies to outline the framework that staff has to take into account when exercising their responsibilities (CEIOPS, *Advice for Level 2 Implementing Measures on Solvency II: System of Governance*, October 2009, p. 12, para 3.67, available at https://eiopa.europa.eu/CEIOPS-Archive/).

[47] FSB provides a useful summary of the key principles of risk governance as follows starting from a stronger risk oversight at Board level. See FINANCIAL STABILITY BOARD, *Thematic review on risk governance*, 2013, p. 30, available at www.financialstabilityboard.org. See also P. MANES, *Corporate Governance, the Approach to Risk and the Insurance Industry under Solvency II*, in M. Andenas – R.G. Avesani – P. Manes – F. Vella – P.R. Wood (eds.), *Solvency II: A Dynamic Challenge for the Insurance Market*, Il Mulino, 2017, chapter IV, p. 115 ff.

[48] EIOPA, *Final Report on Public Consultation No. 14/017 on Guidelines on system of governance*, available at https://eiopa.europa.eu/, at part 2, n. 2.74 states as follows: "While risk management is the responsibility of the undertaking's AMSB as a whole, the undertaking is expected to designate at least one member of the AMSB to oversee the risk management system on its behalf.".

Furthermore, such a solution is uncertain in the case where an executive or a non-executive director is designated to oversee the risk management system. In the case of an executive, there would be an excessive concentration of power in her hands, because she would be involved in managing the risk strategy and at the same time she should check it. In the case of a non-executive director, there would be a kind of separation in respect to the other non-executive directors and many problems would arise: how would the liability regime of the non-executive director be designated to oversee the risk management system set? How about her remuneration? Probably, a better solution would be to assign this function to a risk management committee in which non-executive directors could better support each other in the fulfilment of their task.

For the rest, risk management consists above all of two main areas: the assessment of the risk appetite (through a description that has to be clear and detailed enough in order to express and reflect the strategic high level of objectives of the AMSB), based on quantitative assessment in terms of risk and capital. Risk appetite will be defined by the appropriate directions of the AMSB. The other feature consists of overall risk tolerance limits that express the restrictions that the undertaking imposes on itself when taking risks, and that has to be "metabolized" and "supported" by the Board. It is worth mentioning that the explanatory text of the EIOPA Guideline 17, dealing with the risk tolerance, allows undertakings to adopt stricter constraints [49]. This option is fully in line with a top-down approach to be followed by the Board.

As usual, the risk management system has to be supported by adequate processes and procedures and internal risk reporting is required to be a continuous process within all levels of the undertaking, and the risk management function has to report to the AMSB on risks that have been identified as potentially material. In relation to the risk management policy, Guideline 18 requires a minimum of policies that the undertaking has to establish [50]. On the one side, the undertaking has to

---

[49] EIOPA, *Final Report on Public Consultation No. 14/017 on Guidelines on system of governance*, available at https://eiopa.europa.eu/, at part 2, n. 2.77.b) states as follows: "Risk tolerance limits" expresses the restrictions the undertaking imposes on itself when taking risks. It takes into account: (i) the relevant constraints that effectively limit the capacity to take risks. These constraints can go beyond the framework of solvency as defined in Solvency II (ii) the risk appetite; (iii) other relevant information (e.g. current risk profile of the undertaking, interrelationship between risks)."

[50] EIOPA, *Guidelines on system of governance*, 28 January 2015, EIOPA-BoS-14/253, available at https://eiopa.europa.eu/, Guideline 18 - Risk management policy states: "The undertaking should establish a risk management policy which at least: a) defines the risk categories and the methods to measure the risks; b) outlines how the undertaking manages each relevant category, area of risks and any potential aggregation of risks; c) describes the connection with the overall solvency needs assessment as identified in the ORSA, the regulatory capital requirements and the undertaking's risk tolerance limits;

define the risk categories and the methods to measure the risks; on the other side, the undertaking has to consider each risk globally in relation to its potential effect. In this regard, stress tests are a crucial tool of the risk assessment process.

A final comment is needed with reference to the absence of a general provision inspired by the principle of proportionality. According to Art. 44 of the Solvency II directive on the risk management system, the EIOPA Guidelines describe each area of risk that the risk-management system has at least to cover: underwriting and reserving risk-management; operational risk-management; reinsurance and other risk-mitigation techniques; asset-liability management; investment risk management and liquidity risk management policy. It is worth noting that both the Solvency II directive and the EIOPA Guidelines do refer to a rather rigid risk-management system that calls back an environment based on the 'one size fits all' principle. The regulator probably wanted insurance companies to keep a homogenous approach to risk-management. Nevertheless, it is doubtful whether this system can be implemented with the same standards by each undertaking in a market comprising companies of a different size and complexity.

## 6. TOWARD AN 'EFFECTIVE' BOARD GOVERNANCE

As a consequence of the financial crisis, supervisors are now adopting a more 'intrusive' approach which is focused on making forward-looking judgments about firms. This proactive attitude also includes the supervision on how the Board agrees and oversees the firm's risk framework. This is a profound change which introduces a 'four-eyes' principle to decision-making and the specific role of signing off the strategic plan and monitoring its execution to managers. Most of the firms that failed during the crisis were typically characterized by a domineering chief executive officer, a dysfunctional Board, individuals without the required technical competence, a weak understanding of the risks and inadequate 'four-eyes' oversight. In a nutshell, good governance increases the probability that good decisions will be made, also because poor governance is a strong lead indicator of more significant problems. Because the management is responsible for running firms and firms fail because of the decisions taken by their Board and management, supervisors are interested in an effective role for the Board of directors [51].

---

d) specifies risk tolerance limits within all relevant risk categories in line with the undertaking's risk appetite; e) describes the frequency and content of regular stress tests and the situations that would warrant ad-hoc stress tests.".

[51] H. SANTS, *Delivering effective corporate governance: the financial regulators role*, Speech by Hector Sants, Chief Executive, FSA at Merchant Taylors' Hall, 24 Apr 2012, available at http://www.fsa.gov.uk/. He observes, *inter alia*, that "Boards must be able to

An effective Board is one which understands the circumstances under which the firm would fail, and constantly asks the relevant 'what if' questions. To do this well, a Board needs to understand its business model, understand and focus on material risks, and challenge the executive on the execution of a strategic plan [52]. With regard to technical skills, the EIOPA Guidelines require that the Board collectively understands and addresses the business, but certainly do not expect every member of the Board to have the same degree of technical knowledge. A diverse Board encourages creativity and is less likely to demonstrate a one-way thinking. This key feature is instrumental to allowing that the management and supervisory function of the management body of an institution interacts effectively. However, any Board, included those that are highly qualified and independent, entirely rely on management for the information they need to fully perform their function. Therefore, any Board should resist the "informational capture" by the chief executive officer and the management.

When dealing with strategic or significant decisions, the management body in its supervisory function should be ready and able to challenge and review critically in a constructive manner propositions, explanations and information provided by members of the management body in its management function. It should also be able to monitor the strategy, the risk tolerance and appetite. Moreover, it should assess whether the policies of the institution are implemented consistently and performance standards are maintained in line with its long-term financial interests and solvency [53]. In this context, the EIOPA Guidelines

---

set a strategy and risk appetite and oversee implementation, but they do not substitute for the role of the executive. Likewise, Supervisors challenge hard and can ask for changes, but they do not substitute for the Board or the Executive". On the role of governance as possible substitute of regulation see I. MACNEIL, *Governance and regulation: resetting the relationship*, Law and Financial Markets Review, 6, 2012, 3, p. 169.

[52] Among corporate scholars the subject has been largely neglected in the academic literature with the exception of P. MARCHETTI – G. SICILIANO – M. VENTORUZZO, *Dissenting Directors*, ECGI Working Paper N° 332/2016, October 2016, available at www.ecgi.org/wp.

See again H. SANTS, *Delivering effective corporate governance: the financial regulators role*, Speech by Hector Sants, Chief Executive, FSA at Merchant Taylors' Hall, 24 Apr 2012, available at http://www.fsa.gov.uk/. He also remarks that "it is the Chair's role to construct and manage a Board that has the appropriate and relevant skills and experience to enable it to function effectively".

[53] EIOPA Guideline 1 - The administrative, management or supervisory body. See par. 1.24. "The administrative, management or supervisory body (hereinafter "AMSB") should have appropriate interaction with any committee it establishes as well as with senior management and with persons having other key functions in the undertaking, proactively requesting relevant information from them and challenging that information when

require that the AMSB interacts with the senior management and key functions – included the audit, compliance, actuarial and risk management – "proactively requesting relevant information from them and challenging that information when necessary". This, in turns, refers to the quality of the debate among the Board members. The meetings often appear to be too well orchestrated. Challenge is usually inadequate, possibly as a result of ineffective leadership styles or, more often, dominant leaders that suppress the debate.

The importance of "constructive challenge" in terms of effective decision-making is a lesson learned from the inquiry in the RBS collapse. In 2009, the decision of the RBS to take over ABN AMRO together with Fortis and Santander was evaluated in a UK Financial Services Authority Report [54], whose conclusions are self-explanatory: "In summary, the Review Team concluded that the judgement of the RBS Board in respect of the ABN AMRO acquisition was not characterised by

---

necessary." and par. 1.25. "At group level the AMSB of the participating insurance or reinsurance undertaking, the insurance holding company or the mixed financial holding company should have an appropriate interaction with the AMSB of all entities within the group that have a material impact on the risk profile of the group, requesting information proactively and challenging the decisions in the matters that may affect the group.".

[54] FINANCIAL SERVICES AUTHORITY, *The failure of the Royal Bank of Scotland*, December 2011, p. 228, available at www.fsa.gov.uk/rbs. The Report observes the following: "With reference to the acquisition of ABN AMRO, the Review Team attached special significance to three closely related factors that may have influenced the quality of the RBS Board's decision-making: … it was not apparent to the Review Team that the Board discussed in sufficient depth the risks involved in the acquisition, including its exceptional complexity, unprecedented scale and how it was to be financed, especially as so little effective due diligence was possible. The Board drew comfort from the fact that the limited due diligence, which seems to have focused on identifying the scope for synergies and cost cutting, with less emphasis on identifying the risks and potential exposures, identified no 'show-stoppers' in particular business or functional areas. In the absence of detailed due diligence, the Board also placed reliance on the fact that ABN AMRO was regulated by the DNB and the FSA, on ABN AMRO's publicly available SEC filings, on Sarbanes-Oxley conformity, on reports by the rating agencies and on Barclays' persistence in pursuing its bid- The minutes of the Board meeting on 28 March 2007 record that the RBS CEO '*provided background to the project... A bid for [ABN AMRO] was not seen as a "must do" deal*'. The CEO advised the Board that '*execution risk would be high*' and that '*any bid for [ABN AMRO] and subsequent integration would be more difficult than previous transactions*'. However, the Review Team has not found evidence that the Board undertook any penetrating analysis of the risks on an enterprise-wide basis in respect of capital and liquidity. During interviews with the Chairman and other Board members, it was indicated that, while the assumptions and plans were discussed on a regular basis, '*...at no stage did any Board member propose that we should not proceed*'. One former Board member reflected, with hindsight, that there was an element of 'group-think' in the Board's decision to acquire ABN AMRO and that, to his knowledge, no Board member ever said that he or she was worried about the deal. In the opinion of the Review Team, it is very difficult to reconcile this approach with the degree of rigorous testing, questioning and challenge that would be expected in an effective Board process dealing with such a large and strategic proposition.".

the degree of moderation and sensitivity to strategic risk appropriate to a bank. With so much at stake, there was a critical need for more fundamental probing, questioning and challenge by the Board".

Therefore, in keeping with the emphasis of the financial regulation on the decision-making process, the EIOPA Guidelines state that 'challenge' – on the basis of accurate information – is essential to effective decision-making [55]. Unfortunately, a useless discussion has grown around the word 'challenge'. This rule does not intend to originate a conflict between the Board and the chief executive officer or between non-executives and the executive, but only to underline that ultimately the Board has to make a unitary decision after a constructive debate. It is crucial that such result is conceived after a proper debate about pros and cons of various scenarios – e.g. negative, neutral, positive – and an assessment of all the risks originating from any decision. The chair of the Board needs to stimulate an environment where this is valued. From this perspective, it is clear that 'challenge' should be interpreted as an attitude to understanding the issues and enhancing the quality of the decision through an open-minded debate, supported by diversity of skills, experience and background.

The Board should take a forward-looking judgment in overseeing the running of the firm. In pursuing this task, a good constructive challenge from non-executives improves the quality of the discussion. On the contrary, an annoyed reaction on the part of the chief executive officer or the senior executives would be the sign of a negative attitude. A 'four-eyes' principle to decision-making requires to challenge the executive in all aspects of the firm's strategy, which includes the viability and sustainability of the business model and the establishment, maintenance and use of the risk appetite and management framework. A Board may perform in such effective style only if, on the one side, the executives are

---

[55] A prominent experience on supervisory evaluation of decision making process is a distinctive feature of the Dutch Prudential Supervisor: "DNB's supervision of behaviour and culture considers balanced and consistent decision making as two essential building blocks of an institution's effectiveness … The relevance of balanced and consistent decision making is based on three assumptions. The first of these is that financial institutions can only achieve solid long-term performance and financial performance by carefully considering the interests of all stakeholders. Second, balanced decision making prevents that decisions are taken prematurely and based on incorrect or incomplete information and assumptions. And finally, institutions have to be constantly aware of possible changes in the environment in which they operate. They must adapt to these changes to remain successful. It is important that Board members create a clear and shared understanding about the institution's environment, its "fit" with this environment (…), and how to adapt to changing circumstances (…). Such accurate shared mental models help Boards to adapt to changing circumstances and lead to effective and efficient coordinated management of group behavior.". See DE NEDERLANDSCHE BANK, *Supervision of Behaviour and Culture Foundations, practice & future developments*, November 2015, p. 108, available at https://www.dnb.nl/.

capable of explaining in simple and transparent terms these complex matters to non-executives and, on the other side, the executives try to understand the uncertainty around judgements, in what circumstances they could be wrong, and how different ways may be reasonably adopted to measure the Own Self Risk Assessment and, last but not least, the Internal Risk Model [56]. In pursuing an open and fair confrontation, the Board can prove to be effective.

At the heart of the role of the Board is the setting establishment, maintenance and use of the risk appetite and management framework through the ORSA process. According to EIOPA it is crucial that the Board is aware of all material risks the undertaking faces, regardless of whether the risks are captured by the Solvency Capital Requirement calculation and whether they are quantifiable or not.

As noted by Solvency II experts, the Board should view the ORSA as "an annual process or cycle, rather than just a document or report" [57]. The Board should initially be involved in directing the process and deciding how the assessment is to be performed. The "ORSA should inform discussion between the Board and senior management with regard to the undertaking's risk appetite and how best to deal with risk exposures that may breach the undertaking's capital requirements under its own solvency assessment" [58]. It is also crucial that the Board takes an

---

[56] A. BAILEY, *Governance and the role of Boards*, Speech by Andrew Bailey at Westminster Business Forum, London, 3 November 2015, available at http://www.bankofengland.co.uk/. A Board is required to assess the key elements of model design, the significant assumptions, the expert judgements, the key sensitivities of the internal model, the significant limitations of and the uncertainty in the internal model. According to Bailey, "the challenge is to reduce complexity to simplicity, so that Board members feel that they understand where is the model expected to work well; in what circumstances is it likely to break down; if is the overall model output credible; what are the drivers in terms of key assumptions or judgements; if those assumptions and judgements are reasonable. Non-Executives should be put in a position to possess a general understanding of the model and meet these expectations without detailed technical knowledge. That's the job of the Executive, to explain complexity, provide good management information and enable challenge and thus accountability.".

[57] D. LAVELLE – A. O'DONNELL – D. PENDER - D. ROBERTS – D. TULLOCH, *The Solvency II ORSA Process,* Society of Actuaries, November 2010, Ireland, available at https://web.actuaries.ie/.

[58] S. CLARKE- E. PHELAN, *Stepping stones to ORSA: Looking beyond the preparatory phase of Solvency II*, Milliman Research Report, August 2015, p. 18, available at http://www.milliman.com/. The Report observes the following: "These discussions should influence the strategic decision making of the undertaking and may lead to changes in the undertaking's business plan. For example, risk management techniques such as reinsurance or hedging programmes may be introduced where the ORSA indicates risk exposures that are in excess of the Board's risk appetite. Alternatively, the assessment of overall solvency needs may show that the undertaking has a significant amount of own funds in excess of its overall solvency needs and the Board may decide to issue a dividend as a result, provided that is has the distributable earnings to do so without impacting on

active role. Moreover, "directing the process and challenging the results" of the ORSA should enable the Board to review the developments and achievements [59]. If the Board is not satisfied with the ORSA, it may advise the senior management to take an alternative view in the ORSA process more adequate for the business and risk profile of the insurance undertaking [60].

The EIOPA Guidelines specifically state that the "challenge" process performed by the Board should be documented. Throughout the year, the minutes of the Board meetings, including any remarks and comments relating to the ORSA, should be clearly traceable. Such documentation can then be used to give evidence of the Board's involvement in the process. The approval of the ORSA absolutely requires the active involvement of the Board in the drafting process, as "it would be difficult for the Board to stand over the formal approval of a process that it has not fully engaged with along the way" [61]. The ORSA process needs to gradually become more embedded within the undertaking's business planning process, as the senior management begins to see the benefits, and the Board and senior management need time to become completely comfortable with the process [62].

---

the undertaking's liquidity position. Such discussions and decisions should also be recorded and documented.".

[59] EIOPA, *Guidelines on Own Risk and Solvency Assessment*, 28 January 2015, available at https://eiopa.europa.eu/. See "Guideline 2 – Role of the AMSB: top-down approach. 1.14. The AMSB should take an active part in the ORSA, including steering, how the assessment is to be performed and challenging the results.".

[60] EIOPA, *Guidelines on Own Risk and Solvency Assessment*, 28 January 2015, available at https://eiopa.europa.eu/. See Explanatory text on Guidelines on own risk and solvency assessment par 2.11 "The AMSB challenges the identification and assessment of risks, and any factors to be taken into account. It also gives instructions on management actions to be taken if certain risks were to materialise." and 2.12 "As part of the ORSA the AMSB challenges the assumptions behind the calculation of the SCR to ensure they are appropriate in view of the assessment of the undertaking's risks.".

[61] S. CLARKE- E. PHELAN, *Stepping stones to ORSA: Looking beyond the preparatory phase of Solvency II*, Milliman Research Report, August 2015, p. 18, available at http://www.milliman.com/. See also M. DREHER, *Treatise on Solvency II*, Springer, 2015, at chapter 5, explaining the ORSA process from a legal perspective with special reference to the principle of materiality and proportionality as shaped by the Solvency II directive. As stated at p. 178, "The business strategy of an insurance undertaking thus becomes (…) the indirect subject-matter of supervisory review. In the light of this, and in order to maintain the sole responsibility of the management bodies and the supervisory exemption of the management tasks of the managing board, the supervisory review of ORSA requires particular sensitivity and restraint".

[62] EIOPA, *Guidelines on Own Risk and Solvency Assessment*, 28 January 2015, available at https://eiopa.europa.eu/. See "Guideline 4 – Policy for the ORSA - 1.16. The AMSB of the undertaking should approve the policy for the ORSA. This policy should include at least a description of: a) the processes and procedures in place to conduct the ORSA; b) the link between the risk profile, the approved risk tolerance limits and the overall

The facts and figures of the ORSA should enable the Board to advance its understanding of the risks that the undertaking is exposed to and any changes to risk exposures on a continuous basis. Therefore, the flow of data and information directed to the Board has to be sufficiently detailed to enable it to use them in its strategic decision-making activity. As stated by the EIOPA Guidelines, the ORSA is a very important tool for the Board, as it provides it with a comprehensive picture of the risks the undertaking is exposed to or could face in the future. It has to enable the Board to understand these risks and how they translate into capital needs, or alternatively require risk mitigation techniques. In line with this process, taking into account the insights gained from the ORSA, the Board also approves the long and short-term capital planning, whilst considering the business and risk strategies it has decided upon for the undertaking [63]. This plan includes alternatives to ensure that capital requirements can be met even under unexpectedly adverse circumstances.

## 7. ROLE OF THE BOARD ASSURING A 'FAIR TREATMENT' OF CUSTOMERS

During the financial crisis, many national authorities observed a significant number of instances in which products did not fit the customer's profile or meet the expectations of the customers. They also reported about cases where product provided a very limited coverage excluding main risks to which policyholders were typically exposed. This was reflected in the confidence in insurance firms and products across the sector. Defective products may also affect financial stability, if sold on a mass scale. Moreover, in the current peculiar era of low interest rates, the insurance industry has evolved to design products aimed at purposes beyond mere risk coverage, e.g. investment and money saving. As a consequence, insurance products and contracts tend to be more

---

solvency needs; c) the methods and methodologies including information on: (i) how and how often stress tests, sensitivity analyses, reverse stress tests or other relevant analyses are to be performed; (ii) data quality standards; (iii) the frequency of the assessment itself and the justification of its adequacy particularly taking into account the undertaking's risk profile and the volatility of its overall solvency needs relative to its capital position; (iv) the timing for the performance of the ORSA and the circumstances which would trigger the need for an ORSA outside of the regular time-scales.".

[63] P. MANES, *Corporate Governance, the Approach to Risk and the Insurance Industry under Solvency II*, in M. Andenas – R.G. Avesani – P. Manes – F. Vella – P.R. Wood (eds.), *Solvency II: A Dynamic Challenge for the Insurance Market*, Il Mulino, 2017, chapter IV, p. 119 ff.,

complex and shift financial risks that may not be easily perceived by the average customer [64].

Adapting the MiFID style approach to the insurance sector [65], the EIOPA Guidelines on product oversight and governance try to target the product design and put forward requirements for manufacturers and distributors of insurance products [66]. In addition, the guidelines introduce some key elements for the collaboration between manufacturers and distributors, underlining the importance of strengthening the exchange of product-related information. The EIOPA considers that product oversight and governance arrangements play a key role in customer protection, by ensuring that insurance products meet the needs of the target market and thereby mitigate the potential for mis-selling [67].

It is worth noting that an emerging regulatory trend encompasses the role and responsibility of the Board in the monitoring the risk of mis-selling. According to evidence reported to the EIOPA by various national authorities, conduct weaknesses have been widespread not only among

---

[64] ESA, *Joint Committee Report on Risks and Vulnerabilities in the Eu Financial System*, 7 September 2016, p. 7, available at https://esas-joint-committee.europa.eu, observing that "Search for yield, combined with structural shifts in the financial system due to regulatory changes, is likely to promote the further growth of the fund industry, the asset management sector in general and the trend towards unit-linked and market-based products.".

[65] As regards to the interaction between different pieces of EU financial legislation see V. COLAERT, *Mifid II in relation to other investor protection regulation: picking up the crumbs of a piecemeal approach*, in D. Busch and G. Ferrarini, *Regulation of the EU Financial Markets: MiFID II and MiFIR*, Oxford University Press, 2017, chap. 21, and P. MARANO, *The "Mifidization": The Sunset of Life Insurance in the EU Regulation on Insurance?* available at https://ssrn.com/.

[66] On the MiFID requirements about product governance see D. BUSCH, *Product Governance and Product Intervention under MiFID II/MiFIR*, in D. Busch and G. Ferrarini, *Regulation of the EU Financial Markets: MiFID II and MiFIR*, Oxford University Press, 2017, chap. 5.

[67] EIOPA, *Strategy towards a comprehensive risk-based and preventive framework for conduct of business supervision*, 11 January 2016, available at https://eiopa.europa.eu/. See par. 3.4 "Conduct issues not only harm individual consumers, but can have wider prudential impact as seen with the Payment Protection Insurance mis-selling scandal. Indeed, at national level, there are different approaches to addressing conduct risks with differences in priority setting and levels of resources allocated. These divergences in models and practices across the EU only help to reinforce the current fragmented situation. The interrelationship between conduct and prudential issues plays a key part, on the one hand, regarding the - sometimes - conflicting goals and tension between the two, and, on the other hand, the fact that the ultimate objective of a prudential framework such as Solvency II, is the protection of policyholders. Moreover, poor conduct of business – such as mass mis-selling – can have a systemic impact on the market, i.e. contribute to the development of systemic risk. The overall aim of such a conduct of business supervisory framework is to avoid or to become early enough aware of consumer detriment to be still in a position to act.".

the insurance-based financial products, but also in the personal payments insurance. As far the insurance sector is concerned, the EIOPA Guidelines on product oversight and governance arrangements sets the tone from the top and assign an ultimate responsibility to the Board [68]. A governance framework has culture at its heart, which influences the way in which individuals behave [69]. The culture within the insurance firm needs to be set from the top from the Board and senior management. It is paramount that the Board is effectively involved in, and accountable for, promoting good business conduct. Even more, the public supervision of insurance products plays a special role in customers' protection, but is one of the key areas on which the Board needs to focus with a long-term view.

From a supervisory perspective, customer detriment caused by the purchase of unsuitable and/or poorly designed products can either be addressed *ex post*, by product interventions or banning of products causing customer detriment, or *ex ante*, by addressing the product design

---

[68] EIOPA, *Consultation Paper on the proposal for preparatory Guidelines on product oversight and governance arrangements by insurance undertakings and insurance distributors*, EIOPA-CP-15/008, 30 October 2015, available at https://eiopa.europa.eu/. See Guideline 3 - Role of the manufacturer's administrative, management or supervisory body. "The manufacturer's administrative, management or supervisory body should endorse and be ultimately responsible for the establishment, implementation, subsequent reviews and continued internal compliance with the product oversight and governance arrangements.". Article 21 of the IDD introduces product oversight and governance arrangements for manufacturers and distributors of insurance products. Until the transposition and application of the IDD, there is the possibility that insurance products are offered or sold which not have been subject to internal approval processes aiming at minimising the risk of customer detriment resulting from inappropriate products. Furthermore, there is the possibility that Member States have a diverging view on how the new requirements of IDD should be understood and applied in practice resulting in differences in supervisory approaches and legal uncertainty for market participants expected to take preparatory steps for the implementation of the new rules under IDD. As this matter is being addressed by ESMA and EBA, there is also potential for the coexistence of different regulatory / supervisory approaches in the three financial sectors. See also EIOPA, *Final Report on Public Consultation on Preparatory Guidelines on product oversight and governance arrangements by insurance undertakings and insurance distributors*, 6 April 2016, available at https://eiopa.europa.eu/. In the Guideline 1.25 at par. 1.13. EIOPA underlines that "The administrative, management or supervisory body of the insurance undertaking is responsible for the establishment and subsequent reviews of the product oversight and governance arrangements. However, implementing product oversight and governance arrangements should not be understood as introducing a new key function for insurance undertakings. Moreover, these arrangements are not necessarily linked with the risk management, internal audit, actuarial or compliance functions of insurance undertakings, as prescribed by Solvency II.".

[69] IAIS, *Draft Issues Paper on Conduct of Business Risk and its Management*, 17 June 2015, p. 15, available at https://www.iaisweb.org/. IAIS remarks that "In order to mitigate conduct of business risk, a culture of fair treatment needs to be properly reflected in the governance framework and business objectives and strategies and in implementing a governance framework that promotes fair customer outcomes.".

process and selling practices. This is the reason why the Board has to devote special attention to the process of designing the products and deploying a best effort to give proper consideration to the needs of the target market and to prevent a customer detriment [70].

Product oversight and governance arrangements aim to ensure that the consumer interests are taken into consideration throughout the life cycle of a product, namely the process of designing and manufacturing the product, bringing it to the market and monitoring the product once it has been distributed. They are an essential element of the new regulatory requirements under the IDD [71]. Because of their relevance in terms of customer protection, the role and responsibility of the Board are further detailed and specified. In this respect, the Board ensures that the product oversight and governance arrangements are appropriately designed and implemented into the governmental structures of the manufacturer, and may involve any relevant key functions in the establishment and subsequent reviews of the product oversight and governance arrangements.

Notwithstanding the varieties of implementations of the product oversight arrangements within insurance undertakings, it is required that the ultimate responsibility remains at the Board level. This is made

---

[70] G. BERNARDINO, *Insurance distribution in a challenging environment*, Speech at the European Federation of Insurance Intermediaries (BIPAR), Brussels, 4 June 2015, p. 7, available at https://eiopa.europa.eu/. About the conduct risk regulation and supervision Bernardino underlines as first line of action: “Strengthening corporate governance, i.e. to better integrate conduct of business concerns in the institutional governance arrangements and ensuring that Boards of financial institutions take full responsibility for ensuring that consumer interests are take into account throughout the product lifecycle.”.

[71] EIOPA, *Technical Advice on possible delegated acts concerning the Insurance Distribution Directive*, 1 February 2017, p. 14, available at https://eiopa.europa.eu/. The chapter Role of Management states “21. The administrative, management or supervisory body of the manufacturer or equivalent structure (in the case of two tier systems) is ultimately responsible for the establishment, subsequent reviews and continued compliance of the product oversight and governance arrangements. The manufacturer’s administrative, management or supervisory body also ensures that the product oversight and governance arrangements are appropriately designed and implemented into the governing structures of the manufacturer. 22. The product oversight and governance arrangements, as well as any material changes to those arrangements, are subject to prior approval by the manufacturer’s administrative, management or supervisory body or equivalent structure.”. As well as in relation to insurance distributors EIOPA emphasises that “the ultimate responsibility with regard to the product distribution arrangements lies with the insurance distributor’s administrative, management or supervisory body or equivalent structure even though it is possible that the tasks are delegated either internally or even externally (e.g. in cases of outsourcing). In particular, the ultimate responsibility for the organisational measures and procedures lies with the management of the distributor which is registered and responsible for the distribution activities. For sole traders, it is evident that they bear the responsibility for their entire business.”.

possible by the provision of the EIOPA Guidelines, prescribing that product oversight and governance arrangements, as well as any changes, are subject to prior approval by the manufacturer's AMSB. In fact, the ultimate responsibility of the Board has been considered a sufficient tool in ensuring an effective oversight and responsibility lines over product oversight and governance arrangements of the manufacturer. Ultimately, this requirement reflects the principle of responsibility of the Board in the Solvency II requirements on the system of governance.

## 8. RATINGS AND QUALITY ASSESSMENTS OF CORPORATE GOVERNANCE

Good governance is critical to the long-term sustainability of any company. EU banking and insurance prudential standards require regulated institutions to have a rigorous governance framework, founded on the premise that a well-governed institution is critical to the protection of the interests of depositors and policyholders. The ultimate responsibility for the sound and prudent management of an institution rests with its Board. Key requirements of the prudential standards concern the size and composition of the Board, independence of the chair, and Board renewal and performance assessment. After Solvency II – and possible capital adds-on in case of governance failure [72] –, a formal system to rate the governance of insurance undertakings in the EU must be designed, which could be useful for both the firms and the Supervisors. For instance, a rating is provided by a Supervisory Authority at the event of an on-site inspection on the results of this activity. There is no permanent evaluation of the governance based on a quantitative approach, but only on a single basis on the result of the annual reports.

To build up the rating of the effectiveness of the Board, a common methodology at the European level is needed. In performing these quality assessments, a proportionate approach is paramount to consider the size and complexity of the firm's operations. Looking at the practical aspects of quality assessments, there should be a guide for supervisors by the EIOPA as to how each of these factors should be considered and rated. It should include suggestions for documents and other sources which would help in the quality assessment, and these are used to compile the assessment [73]. They include Board papers and minutes, prudential

---

[72] The capital add-on is a "tool of last resort", as notes M. DREHER, *Treatise on Solvency II*, Springer, 2015, at p. 63, but this does not rule out lesser measures that address violations. He also highlights that "In order to impose a capital add-on, the supervisory authority must convert a qualitative deficiency into a quantitative measure, thus, in a manner of speaking, squaring the circle".

[73] The quality assessment of risk governance addresses various aspects, including the effectiveness of the Board in relation to risk governance, the functioning of the main

consultations, risk reviews, and discussions with the management and Board. To be consistent in the quality assessments of each area and in the ratings of firms, a benchmarking exercise would be useful, given the wide variety of institutions in the European landscape. It is worth noting that the Solvency II Guidelines on the system of governance do not include any peer comparison. The results of any quality assessments of risk governance and the Board effectiveness depend crucially on benchmarking, which would help improve most institutions. Moreover, the development of a methodological framework for corporate governance quality assessment conducted by national competent authorities would be beneficial for the supervisory convergence across the European Union. Best practices should also be identified and made public, with the aim of strengthening the self-discipline of the insurance firms involved.

## 9. REMUNERATION

One of the most prominent issues that has been attracting the attention of different stakeholders is related to the remuneration practices applied to the members of the Board and senior management of financial entities, as well as to personnel undertaking activities that involve risk-taking. Specifically, for insurance firms, remuneration policies that excessively reward short-term profit and give incentives to take risks that are not in line with the undertaking's risk profile can undermine sound and effective risk management, exacerbate excessive risk-taking behaviour and lead to potential conflicts of interest.

Although the majority of these situations occurred in sectors other than the insurance, in the context of the Solvency II regime it was considered that some principles should be applied and preventive measures should be allowed for and implemented by insurance undertakings. Therefore, notwithstanding the absence of any provision in the Directive [74], having considered that an adequate system of

committees (audit, risk and remuneration), the remuneration policy, the risk management framework and the internal control functions. The risk culture should be out of the scope of this assessment, because it is fair to rely on the Board's assessment of the institution's risk culture and the process followed for this assessment. The quality assessment of the Board should consider the following areas: Board charter and self-assessment; the quality, skills and experience of all directors; the Board composition and independence; the fitness and propriety matters; the conflicts of interest policy; the internal control framework and the outsourcing policy.

[74] See Article 275 of the European Commission Delegated Regulation 2015/35. These requirements include the obligation for the establishment and maintenance of remuneration policies and procedures to avoid conflicts of interest and promote sound and effective risk management. The remuneration requirements for the insurance sector is not as prescriptive and detailed as CRD IV, AIFMD or UCITS V.

governance should include the implementation of an appropriate remuneration policy, the Implementing Measures require undertakings to adopt a remuneration policy that is in line with its business strategy and risk profile, and should avoid any potential incentives for unauthorised or unwanted risk-taking [75].

In order to ensure the adequacy of the process, the undertaking's shareholders should be involved in the approval of the remuneration policy with reference to the remuneration of the Board. The latter should define the remuneration applicable to the key functions, senior management, personnel undertaking activities that involve significant risk-taking, and others staff. The remuneration policy should be subject to a regular (at least annual) and independent internal review, with specific attention to preventing incentives for excessive risk-taking and the creation of conflicts of interest between the employees and the undertaking as a whole, and generally not undermining sound and effective risk management. In this review, the appropriateness of the basis on which the variable component of remuneration is set, as well as its proportion, should be assessed, and recommendations should be provided when appropriate.

## 10. FINAL REMARKS

Under EU law, after the CRD IV and Solvency II directives, the prudential authorities operate as supervisors in charge of the application of judgement against a complex and multilevel framework of rules and guidelines which also encompasses the system of governance [76].

---

[75] Although Solvency II and the EIOPA Guidelines are not as prescriptive as CRD IV, they differ in a number of significant ways. First of all, there is more limited scope to dis-apply the remuneration requirements on a proportionate basis, even if Article 275(3) of the Solvency II Regulation provides for the application of the proportionality principle with the internal organisation of the insurance or reinsurance undertaking, and the nature, scale and complexity of the risks inherent in its business. Secondly, it does not limit variable pay deferral to significant bonuses. Third, Article 275(2)(c) of the Solvency II Regulation requires firms to defer a substantial portion of the variable remuneration component for a period of not less than three years. There is no flexibility in the Solvency II Regulation to prefer a shorter period than the three-years period. Firms are required to ensure that the period (three years or longer) is correctly aligned with the nature of the business, its risks, and the activities of the employees in question. Deferral of variable remuneration allows firms to apply downwards adjustments, in particular by application of the malus (during the three-years deferral period) prior to the award vesting, to take account of specific risk management failures. The wording in the Solvency II Regulation is identical to the text of the CRD, which applies to banks, building societies and investment firms, even though the latter includes a specific 40% minimum deferral threshold.

[76] Prudential regulations should abstain from setting too detailed requirements as to the organization and functioning of Boards: see G. FERRARINI, *Understanding the Role of*

Conversely, the regulation of corporate governance should be based on a limited number of standards, with which Boards should comply under the *ex post* supervision of supervisory authorities. A similar approach is preferable to the extent that it is respectful of the autonomy of insurance undertakings, while leaving supervisors with the "effectiveness" of corporate governance from the perspective of the safety and soundness of the institutions concerned. Narrow rule-based approaches to regulations create inflexibility and can easily lead to arbitrage [77]. In the context of the European Union, it will depend on the European Supervisory Authorities whether to continue having regulations of the highest standards on corporate governance, which sort out a fair relationship between harmonisation and reliability, but a more principle-based regulation should be developed under a common framework of a peer-review of supervisory practice – both at national and European level – within European cross-sectoral metrics of quality assessment.

The regulation has a deep influence on the development of the risk culture, risk management, and internal control systems. However, understanding how firms take and manage risk and the controls they perform is at the heart of the job of a Board. The standards of this work have been increased since the crisis, which was probably necessary also in corporate governance as a whole. However, it remains to be seen if the exceptional extension of the duties and responsibilities assigned to the Board of directors, far beyond the traditional role both of monitoring the chief executive officer and assessing the overall direction and strategy of the business, will be successful in achieving a better risk governance.

Furthermore, it seems that insurance regulation has a twofold approach to corporate governance issues: on the one side, it endorses criteria traditionally adopted in the European context; on the other side, it enacts specific rules and procedures that already characterize the corporate governance in the banking sector. European insurance regulation should aim to create a more flexible corporate governance structure, with particular emphasis to the additional duties of the Board of directors or to the risk-management requirements established in the Level 3 Guidelines. In both cases, they do not seem to fully endorse the proportionality principle, since they require a 'one size fits all' risk-

---

*Corporate Governance in Financial Institutions: A Research Agenda*, Law Working Paper n. 347, 2017, available at www.ecgi.org/wp. Moreover, various regulatory provisions "petrify existing corporate governance best practices" as state L. ENRIQUES - D. ZETSCHE, *Quack Corporate Governance, Round III? Bank Board Regulation Under the New European Capital Requirement Directive*, Theoretical Inquiries in Law, 16.1, 2015, p. 211, at p. 240.

[77] A. BAILEY, *Governance and the role of Boards*, Speech by Andrew Bailey at Westminster Business Forum, London, 3 November 2015, available at http://www.bankofengland.co.uk/.

management structure for every insurance undertaking, irrespective of the size, business model and whatever essential characteristics. A possible explanation is that European insurance regulation aims to adopt a strict regulatory framework for these aspects, believing that they deserve particular attention because of their crucial role in enhancing corporate governance. This approach can be useful for fostering corporate governance culture, although procedures can sometimes be either too broad or too narrow tools for any undertaking.

Regulators must play an active role in ensuring that insurance undertakings have in place the right governance and culture [78]. But it is not up to the supervisor to determine the culture, business strategy or remuneration policy. The right cultures are rooted in strong ethical frameworks and in the importance of individuals making decisions in relation to principles, rather than only business-oriented values. However, there is room for conflicting views between the regulator and the firms, given the natural short-terminims of management [79]. In the middle – or, one could say, in the firing line – stands the Board.

The crisis revealed significant failures in the governance and risk management of financial firms – although the insurance sector proved to be involved only to a limited extent –, as well as their underlying culture and ethics. These deficiencies are not so much a "structural" issue, but are rather the result of conducts, attitudes and, in some cases, competence of the Boards and senior management. Indeed, "more work remains: national authorities need to strengthen their ability to assess the effectiveness of a firm's risk governance, and more specifically its risk culture, to help ensure sound risk governance through changing

[78] Managerial and supervisory attention should be paid to ensure that culture and remuneration structures support risk management in financial institutions. As risk culture varies at the local level, it should be measured and managed at the local level. Senior leaders cannot rely on their own perceptions; rather, they should rely on independent assessments of risk culture: see E. SHEEDY- B. GRIFFIN, *Risk governance, structures, culture, and behavior: A view from the inside*, Corp Govern Int. Rev. 2017, available at https://doi.org/10.1111/corg.12200. See also L. REDMOND, *Risk Culture: A View from the Board*, in P. Jackson (ed.), *Risk Culture and Effective Risk Governance*, Risk Books, 2014, chapter 3, p. 47 ff.

[79] In banking and regulation literature, there is still meagre attention to the diffusion of governance principles that impact longer-term performance, with the exception of the following: M. MOSCHELLA - E. TSINGOU, *Regulating finance after the crisis: unveiling the different dynamics of the regulatory process*, Regulation and Governance, 7, 2013, p. 407 and T. RIXEN, *Why reregulation after the crisis is feeble: shadow banking, offshore financial centers, and jurisdictional competition*, Regulation and Governance 7, 2013, p. 435.

environments” [80]. Boards should promote an ethical culture, in which challenges can be openly expressed.

Risk governance, inclusive of risk culture, is a relatively new approach to the corporate governance of both insurance firms and other financial institutions; it implies a crucial role for the Board, pushing towards a strategy of effectiveness of risk structures and risk culture within the firm, and opens up new challenges for the supervisor, during the assessment and comparison of the results across the industry [81]. A responsive, yet not intrusive, regulation would be even more helpful.

## REFERENCES

A. BAILEY, *Governance and the role of Boards*, Speech by Andrew Bailey at Westminster Business Forum, London, 3 November 2015, available at http://www.bankofengland.co.uk/.

ARMOUR J. – AWREY D. – DAVIES P.L. – ENRIQUES L. – GORDON J.N. – MAYER C. – PAYNE J., *Bank Governance*, ECGI Working Paper N°. 316/2016, June 2016, available at www.ecgi.org/wp.

ARNDORFER I. – MINTO A., *The "four lines of defence model" for financial institutions*, BIS Financial Stability Institute, Occasional Paper n. 11, 2015, p. 3, available at http://www.bis.org/fsi/.

BASEL COMMITTEE ON BANKING SUPERVISION, *Principles for enhancing corporate governance*, 2010, available at www.bis.org.

BELTRATTI A. –STULZ R.M., *Why did some banks perform better during the credit crisis? A cross-country study of the impact of governance and regulation*, Journal of Financial Economics 105, 2012, p. 1.

BERNARDINO G., *Insurance distribution in a challenging environment*, Speech at the European Federation of Insurance Intermediaries (BIPAR), Brussels, 4 June 2015, p. 7, available at https://eiopa.europa.eu/.

---

[80] FINANCIAL STABILITY BOARD, *Thematic review on risk governance*, 2013, p. 1, available at www.financialstabilityboard.org.

[81] In response to the financial crisis, the Dutch prudential supervisor decided to include aspects of behaviour and culture into its supervisory approach. See DE NEDERLANDSCHE BANK, *Supervision of Behaviour and Culture Foundations, practice & future developments*, November 2015, available at https://www.dnb.nl/. The ECB is even more interested in corporate governance. In 2016, the issue of internal governance was one of the top supervisory priorities of the Single Supervisory Mechanism (SSM) and one of the key elements of the Supervisory Review and Evaluation Process (SREP) on an annual basis. It is worth noting that a key recommendation states as follows: “Boards should challenge, approve and oversee the management’s implementation of the bank’s strategic objectives, governance and corporate culture”: see EUROPEAN CENTRAL BANK, *SSM supervisory statement on governance and risk appetite*, June, 2016, p. 2, available at https://www.bankingsupervision.europa.eu/ecb/.

BOUBAKRI N., *Corporate governance and issues from the insurance industry*, Journal of Risk and Insurance, 78, 2011, 3, p. 501.

BUSCH D., *Product Governance and Product Intervention under MiFID II/MiFIR*, in D. Busch and G. Ferrarini, *Regulation of the EU Financial Markets: MiFID II and MiFIR*, Oxford University Press, 2017, chap. 5.

CEIOPS, *Advice for Level 2 Implementing Measures on Solvency II: System of Governance* (former Consultation Paper 33), October 2009, p. 3, available at https://eiopa.europa.eu/CEIOPS-Archive/.

CEIOPS, *Advice to the European Commission on the Principle of Proportionality in the Solvency II Framework Directive proposal*, CEIOPS-DOC-24/08, May 2008, available at https://eiopa.europa.eu/CEIOPS-Archive/.

CHEFFINS B., *The Corporate Governance Movement, Banks and the Financial Crisis*, *Theoretical Inquiries in Law*, vol. 16 n.1, 2015, p.1.

CLARKE S. - PHELAN E., *Stepping stones to ORSA: Looking beyond the preparatory phase of Solvency II*, Milliman Research Report, August 2015, available at http://www.milliman.com/.

COLAERT V., *Mifid II in relation to other investor protection regulation: picking up the crumbs of a piecemeal approach*, in D. Busch and G. Ferrarini, *Regulation of the EU Financial Markets: MiFID II and MiFIR*, Oxford University Press, 2017, chap. 21,

CONFERENCE OF INSURANCE SUPERVISORY SERVICES OF THE MEMBER STATES OF THE EUROPEAN UNION, *Prudential supervision of insurance undertakings*, Report prepared under chairmanship of Paul Sharma, 2002, available at http://ec.europa.eu/internal_market/insurance/.

DE JAGER C. E., *A Question of Trust: the Pursuit of Consumer Trust in the Financial Sector by Means of EU Legislation*, J. Consumer Policy, 40, 2017, p. 25, at p. 24.

DE LAROSIÈRE HIGH LEVEL GROUP, *Report on the future of financial supervision in the EU*, 25 February 2009, Brussels.

DE NEDERLANDSCHE BANK, *Supervision of Behaviour and Culture Foundations, practice & future developments*, November 2015, p. 108, available at https://www.dnb.nl/.

DREHER M., *Treatise on Solvency II*, Springer, 2015.

EBA, *Draft Guidelines on internal governance*, Consultation Paper, 28.10.2016, available at https://www.eba.europa.eu

EIOPA, *Consultation Paper on the proposal for preparatory Guidelines on product oversight and governance arrangements by insurance undertakings and insurance distributors*, EIOPA-CP-15/008, 30 October 2015, available at https://eiopa.europa.eu/.

EIOPA, *Final Report on Public Consultation No. 14/017 on Guidelines on system of governance*, available at https://eiopa.europa.eu/.

EIOPA, *Final Report on Public Consultation on Preparatory Guidelines on product oversight and governance arrangements by insurance undertakings and insurance distributors*, 6 April 2016, available at https://eiopa.europa.eu/.

EIOPA, *Guidelines on Own Risk and Solvency Assessment*, 28 January 2015, available at https://eiopa.europa.eu/.

EIOPA, *Guidelines on system of governance*, 28 January 2015, EIOPA-BoS-14/253, available at https://eiopa.europa.eu/.

EIOPA, *Strategy towards a comprehensive risk-based and preventive framework for conduct of business supervision*, 11 January 2016, available at https://eiopa.europa.eu/.

EIOPA, *Technical Advice on possible delegated acts concerning the Insurance Distribution Directive*, 1 February 2017, p. 14, available at https://eiopa.europa.eu/.

ENRIQUES L. - ZETSCHE D., *Quack Corporate Governance, Round III? Bank Board Regulation Under the New European Capital Requirement Directive*, Theoretical Inquiries in Law, 16.1, 2015, p. 211, at p. 240.

ERHARD W. – JENSEN M., *Putting integrity into finance: a purely positive approach*, ECGI Finance Working Paper, last rev. 2015, 417, Appendix 1, available at http://www.ecgi.org.

ESA 3L3 TASK FORCE ON INTERNAL GOVERNANCE, *Cross-sectoral stock-take and analysis of internal governance requirements*, October 2009, available at https://www.eba.europa.eu.

ESA, *Joint Committee Report on Risks and Vulnerabilities in the Eu Financial System*, 7 September 2016, available at https://esas-joint-committee.europa.eu.

ESMA – EBA, *Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU*, Consultation Paper, 28.10.2016, available at https://www.esma.europa.eu/.

EUROPEAN CENTRAL BANK, *SSM supervisory statement on governance and risk appetite*, June, 2016, p. 2, available at https://www.bankingsupervision.europa.eu/ecb/.

EUROPEAN COMMISSION, *Green Paper, Corporate governance in financial institutions and remuneration policies*, COM (2010), 284 final, available at http://ec.europa.eu/internal_market/.

EUROPEAN COMMISSION, *Green Paper, Corporate governance in financial institutions and remuneration policies*, COM (2010), 284 final.

EUROPEAN SYSTEMIC RISK BOARD, *Report on misconduct risk in the banking sector*, June 2015, available at https://www.esrb.europa.eu/.

FERRARINI G., *Understanding the Role of Corporate Governance in Financial Institutions: A Research Agenda*, Law Working Paper n. 347, 2017, available at www.ecgi.org/wp.

FINANCIAL SERVICES AUTHORITY, *The failure of the Royal Bank of Scotland*, December 2011, p. 228, available at www.fsa.gov.uk/rbs.

FINANCIAL STABILITY BOARD, *Guidance on supervisory interaction with financial institutions on risk culture*, April 2014, available at http://www.fsb.org/

FINANCIAL STABILITY BOARD, *Thematic review on risk governance*, 2013, available at www.financialstabilityboard.org.

G20/OECD, *Principles of Corporate Governance*, 2015, available at http://www.oecd.org/.

GROUP OF THIRTY, *Banking conduct and culture: a call for sustained and comprehensive reform*, July 2015, available at http://group30.org

GUCCIONE A.V., *From Solvency to Omnibus. Historical Origins and Normative Evolution*, in M. Andenas – R.G. Avesani – P. Manes – F. Vella – P.R. Wood (eds.), *Solvency II: A Dynamic Challenge for the Insurance Market*, Il Mulino, 2017, chapter I, p. 35.

HILB M., *Redesigning corporate governance: lessons learnt from the global financial crisis*, Journal of Management and Governance, v. 15 n.4, 2011, p. 533.

HOPT K., *Corporate Governance of Banks and Other Financial Institutions after the Financial Crisis*, J. Corp. L. Studies, 2013, p. 237.

IAIS, *Draft Issues Paper on Conduct of Business Risk and its Management*, 17 June 2015, p. 15, available at https://www.iaisweb.org/.

KIRKPATRICK G., *The corporate governance lessons from the financial crisis*, Financial Market Trends, 2009, 3(1), available at http://search.oecd.org/finance/financial-markets/.

KPMG, *Study into the methodologies to assess the overall financial position of an insurance undertaking from the perspective of prudential supervision*, May 2002, available at http://ec.europa.eu/internal_market/insurance/.

LAVELLE D. – O'DONNELL A. – PENDER D. - ROBERTS D. – TULLOCH D., *The Solvency II ORSA Process,* Society of Actuaries, November 2010, Ireland, available at https://web.actuaries.ie/.

LEVINE R., *The corporate governance of banks: a concise discussion of concepts and evidence*, World Bank Policy Research Working Paper, n. 3404, 2004, available at http://documents.worldbank.org/

MACNEIL I., *Governance and regulation: resetting the relationship*, Law and Financial Markets Review, 6, 2012, 3, p. 169.

MANES P., *Corporate Governance, the Approach to Risk and the Insurance Industry under Solvency II*, in M. Andenas – R.G. Avesani – P. Manes – F. Vella – P.R. Wood (eds.), *Solvency II: A Dynamic Challenge for the Insurance Market*, Il Mulino, 2017, chapter IV, p. 93.

MARANO P., *The "Mifidization": The Sunset of Life Insurance in the EU Regulation on Insurance?* available at https://ssrn.com/.

MARCHETTI P. – SICILIANO G. – VENTORUZZO M., *Dissenting Directors*, ECGI Working Paper N° 332/2016, October 2016, available at www.ecgi.org/wp.

MOLONEY N., *EU Securities and Financial Markets Regulation*, 2014, p. 357.

MOSCHELLA M. - TSINGOU E., *Regulating finance after the crisis: unveiling the different dynamics of the regulatory process*, Regulation and Governance, 7, 2013, p. 407

MULBERT P.O., *Corporate Governance of Banks*, European Business Organisation Law Review, v.11 n.3, 2008, p. 427

OECD STEERING COMMITTEE ON CORPORATE GOVERNANCE, *Corporate governance and the financial crisis*, available at http://www.oecd.org/.

PI L. - TIMME S.G., *Corporate control and bank efficiency*, Journal of Bank and Finance, vol. 17 n.2-3, 1993, p. 515

R.D. CITLAU – MÜLBERT P.O., *The uncertain role of banks' corporate governance in systemic risk regulation*, ECGI Law Working Paper n. 179, 2011, available at www.ecgi.org/wp.

REDMOND L., *Risk Culture: A View from the Board*, in P. Jackson (ed.), *Risk Culture and Effective Risk Governance*, Risk Books, 2014, chapter 3, p. 47.

RICCI O., *Corporate Governance in the European Insurance Industry*, Springer, 2014.

RIXEN T., *Why reregulation after the crisis is feeble: shadow banking, offshore financial centers, and jurisdictional competition*, Regulation and Governance 7, 2013, p. 435.

SANTS H., *Delivering effective corporate governance: the financial regulators role*, Speech by Hector Sants, Chief Executive, FSA at Merchant Taylors' Hall, 24 Apr 2012, available at http://www.fsa.gov.uk/.

SHEEDY E. - GRIFFIN B., *Risk governance, structures, culture, and behavior: A view from the inside*, Corp Govern Int. Rev. 2017, available at https://doi.org/10.1111/corg.12200.

SWAIN R. – SWALLOW D., *The prudential regulation of insurers under Solvency II*, Bank of England, Quarterly Bulletin 2015 Q2, p. 145, available at http://www.bankofengland.co.uk/.

VAN DER ENDE J. – AYADI R., *Insurance Regulation and Supervision in the EU: Report of a CEPS Task Force*, Brussels, 2006

VAN HULLE K., *The challenge of Solvency II: Lecture to the faculty of actuaries*, British Actuarial Journal, 2008, 14, 1, p. 27.

WINTER J., *The Financial Crisis: Does Good Corporate Governance Matter and How to Achieve it?* in E. Wymeersch, K.J. Hopt, and G. Ferrarini (eds.), *Financial Regulation and Supervision. A post-crisis analysis*, 2012, para. 12.

WRIGHT S. – SHEEDY E. – MAGEE S., *International compliance with new Basel Accord principles for risk governance*, Account. Finance, 2016, available at https://doi:10.1111/acfi.12213.