ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 640 FINANSE, RYNKI FINANSOWE, UBEZPIECZENIA NR 38 2011

MARIA KIEDROWSKA
ELŻBIETA IZABELA SZCZEPANKIEWICZ

INTERNAL CONTROL IN THE CONCEPT OF INTEGRATED ENTERPRISE RISK MANAGEMENT (ERM) SYSTEM IN INSURANCE UNDERTAKINGS

Introduction

Faced with the risk of consecutive waves of financial crisis and economic recession, government committees, financial supervision authorities and financial institutions themselves – both in Poland and worldwide – have launched a number of measures to make the supervision of insurance companies more effective, particularly in aspects related to efficient risk management and internal control.

Due to high social and economic importance, the activities of institutions operating in the insurance sector are subject to mandatory financial supervision. Insurers are obliged to comply with a range of requirements, introduced as far back as 1973, which are aimed at securing the safety of their business operations. One of the basic requirements applicable to the insurance business is solvency. An important step to improve the system of solvency assessment in institutions was the introduction of Solvency I. Economic globalization, coupled with the worldwide disclosure of irregularities and frauds in a number of major financial institutions sparked a debate on changes in the solvency regime of these entities. The discussion was initiated by the European Commission in 2001. A number of risk analyses' were performed to assess key risks inherent in the insurance and reinsurance sector. Bankruptcies were discussed, as well as existing solvency models implemented in various countries. Following the USA's announcement of SOX[1], in December 2002 the European Commission adopted Directive 2002/87/EC on the **supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate.** Guidelines enacted in 1970–2000 were amended, and new legislation was passed – including Directive 2002/83/EC concerning life assurance, and Directive 2005/68/EC on reinsurance. The year

[1] In 2002 the USA authorized the establishment of effective and adequate internal control systems, their monitoring by management boards and assessment by independent auditors in public companies (that is, in the majority of financial institutions) by enacting the Sarbanes Oxley Act (SOX). Before that, the role and scope of internal control was regulated by the *COSO Report* (Internal Control – Integrated Framework), COSO II Report (Enterprise Risk Management – Integrated Framework) and The International Standards for the Professional Practice of Internal Audit.

2006 saw the announcement of Directive 2006/43/EC which laid down guidelines for the development of further national regulations on the supervision of entities auditing financial statements of enterprises (employing certified auditors). The Directive contained provisions requiring public-interest entities to establish audit committees and introduced the obligation to assess internal control systems, evaluate the effectiveness of risk management and oversee internal audits. It was not until 2009 that works were completed on a draft of a new solvency regime which was set out in detail in Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II). Solutions adopted pursuant to the Directive must be transposed by Member States into their national laws by 31 October 2012. Amendments included in Solvency II relate to a number of business areas of insurance institutions, including: risk management, implementation of an adequate internal control system and establishment of an internal audit function. Even though the new regulations will not become formally effective until late 2012, insurers must now take appropriate measures to adapt the accounting policy, risk analysis methods and risk management, reporting and IT systems to the new regulations.

This article seeks to outline the Author's own management system model comprising integrated risk management and internal control in insurance undertakings, based on the Polish regulations in force and Solvency II.

Governance and supervision system in insurance undertakings in the light of Polish regulations and Solvency II

Many financial institutions operating in Poland implemented internal control systems several years ago. They also established internal audit functions and audit committees. The pioneers in this field were banks and brokerage firms. Following the example of banks, some of the insurance companies took similar actions. Recent legislative amendments, however, imposes a set of formal obligations on insurance companies, requiring them to:

- set up an audit committee to assess the institution's internal control and risk management systems, and supervise internal audit activities, if an appropriate function has already been established in the institution (Art. 86 of the Act on Statutory Auditors, 2009),
- develop and implement principles governing risk acceptance and the internal control system (Art. 93 of the Act on the Insurance Business, 2010).

Insurers should regard the above activities are a preparation for the implementation of guidelines laid down in Solvency II (2009). It needs to be stressed that the new governance and supervision system regime applicable to the insurance sector required under Solvency II is more complex than any previous regulations in force. It is based on three main pillars aimed at securing the institution's operations, encompassing quantitative (capital-related), qualitative and reporting requirements. Areas regulated under PILLAR II complement PILLAR I, as not all risks are measurable exclusively in quantitative terms. Both risks ex-

pressed qualitatively and quantitatively should be subject to special internal and external supervision. This is why the idea of management and supervision system under Solvency II is based on a complex approach to risk management and establishment of internal control systems that are adequate to the defined risk. These two elements make up an integrated system of enterprise risk management (ERM) in the functional sense. However, an effective management and internal control system also requires an internal audit function and an audit committee. The management and control system is also complemented by PILLAR II which contains reporting provisions. Table 1 presents a model of the management and supervision system laid down by Solvency II.

Table 1

Solvency II model of management and supervision system in insurance undertakings

PILLAR I	PILLAR II	PILLAR III
Quantitative requirements (capital) (Art. 75–135)	Qualitative requirements (Art. 27-30, 40–51, 212–217, 248–252)	Reporting requirements (Art. 51–56, 221, 256)
– vlities – technical and insurance reserves, – own funds, – capital-related solvency requirement, – minimum capital requirement, – investment.	1) Operation of supervisory authorities 2) Governance system – risk management, – own risk and solvency assessment, – internal control, – internal audit, – actuarial function, – outsourcing.	1) Public disclosure of information on solvency and financial condition, 2) Information for supervision purposes.

Source: Author's own study based on Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).

It should be noted that the new Solvency II system gives insurers a wider scope of powers in the area of risk estimation and capital adequacy. Therefore, EU Member States have an obligation to demand the introduction of an effective governance system (specified in PILLAR II) from all insurance sector undertakings. The system should ensure sound and prudent management of the undertaking's business and be adjusted to the nature, scale and degree of complexity of the undertaking's activity. The governance system should comprise the following elements:

- risk management,
- internal control procedures,
- internal audit,
- actuarial function.

Insurance and reinsurance undertakings should prepare, and accept for use, a set of written policies governing the organization and functioning of the elements listed above (Art. 41 of Solvency II).

In order to maintain the effectiveness of the risk management system, it needs to be integrated with internal control procedures. The system should also cover reporting strategies, processes and procedures which are necessary for the identification, measurement and monitoring of risks to which they are, or may be, exposed. Undertakings are required to investigate interdependencies between risks on a continuous basis. They should also manage different risk types and report on them accordingly. The risk management system should provide for all existing risks, particularly those that need to be included in calculations of the solvency capital requirement. Under Art. 44, the system should cover at least the following areas:

- underwriting and reserving,
- management of assets and liabilities,
- investment, including derivatives and similar financial instruments,
- liquidity and concentration risk management,
- operational risk management,
- reinsurance and other risk-mitigation techniques.

Introduction of the risk management system requires:

- development and implementation of an internal risk management model,
- testing and validation of the internal model,
- preparation of documentation for the model,
- analysis of the performance of the internal model and preparation of appropriate summary reports,
- notification of the management of the undertaking and the supervisory body about the performance of the internal model (with specification of areas needing improvement), and up-dating on measures taken to improve previously identified weaknesses of the system.

Within the framework of the risk management system, each insurance undertaking performs its own assessment of risk[2] and solvency. The undertaking's own risk and solvency assessment is an integral part of the business strategy and, as such, it should be taken into account in all strategic decisions taken by the undertaking. Under Art. 45, the assessment should include at least the following elements:

- overall solvency needs – taking into consideration the specific risk profile, approved risk tolerance limits and the undertaking's business strategy,

[2] The new model of capital requirements will be based on insurance, market, credit and operational risks. The risk of concentration will be accounted for together with the above-mentioned risk types. The foreign exchange risk will be included in the market risk, just like the solvency risk.

– continuous compliance with requirements concerning relevant capital provisions and technical insurance provisions,

Insurance undertakings are required to have in place an effective internal control system (Art. 46). The system should incorporate administrative and accounting procedures, an internal control framework, reporting arrangements at all levels of the undertaking, and a compliance function. The compliance function is effected by advising the administrative, management or supervisory body on compliance with applicable statutory provisions, executive regulations and administrative provisions adopted under this Directive. It should also include an assessment of possible impact of any changes in the legal environment on the undertaking's operations and the identification and assessment of compliance risk.

The undertaking's management system should be subject to regular internal reviews, performed at least once a year. Therefore, insurance undertakings should also put in place the internal audit function (Art. 47). The internal audit function is responsible for evaluating the adequacy and effectiveness of the internal control system and other elements of the system of governance. Depending on the system adopted by the undertaking concerned, the audit unit may be subordinate to the audit committee (or the supervisory board) or to the undertaking's management board. The internal auditor should report the findings of the internal audit to the management and the supervisory body. However, it is the management body that decides which measures should be undertaken with regard to the findings and recommendations resulting from the internal audit, and ensures that the measures are implemented.

Assuming that the management system in place in the insurance undertaking includes elements presented above, a target model of the integrated risk management and internal control has been developed. The model is presented in Fig. 1.

It should be pointed out that the integrated risk management and internal control system which is subject to the auditor's assessment is developed, implemented, monitored and improved on an ongoing basis by the management and executive of individual organizational units. The auditor's task is to perform periodical independent and objective assessment of the integrated system. The governance and supervision system shown in Fig. 1 assumes that in the undertaking's organizational structure the internal audit function is subordinate to the audit committee (established at the supervisory board). The solution makes it possible to evaluate not only internal control procedures at the operational level, but also to assess decisions taken by the top executive at the managerial level with regard to risk management effectiveness and adequacy. Insurance undertakings, however, can also adopt an alternative solution whereby the internal audit function is directly subordinate to the management board. In this case, the scope of assessment is limited to the investigation of systems at the operational level, which gives the supervisory board a markedly reduced possibility of assessing the undertaking's business.

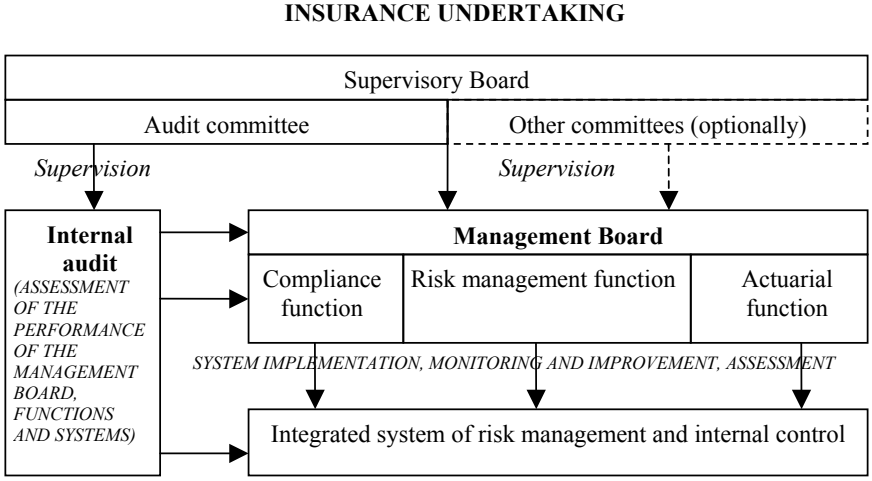

Fig. 1. Target governance and supervision system in Polish insurance undertakings

Source: own work.

Since there is no Polish legislation regulating the development of the risk management and internal control system, insurance undertakings should make use of relevant international standards.

Integrated risk management and internal control system (ERM) in the insurance undertaking in the light of international standards

The basic standards relating to the management of risk and internal control which are followed by insurance enterprises include:

- The COSO Report: Internal Control – Integrated Framework (1992),
- The COSO II Report: Enterprise Risk Management – Integrated Framework (2004),
- The Standard IASA: Standard on Enterprise Risk Management for Capital Adequacy and Solvency Purposes (2008), based on COSO II Report.

The COSO report[3] defines internal control as a process initiated and exercised by the supervisory board, management board, the executive and other staff members to ensure that:

- all operations are effective and efficient,
- financial reporting is reliable,
- regulations and internal rules are followed.

[3] The COSO Report: Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadeway Commision, USA (1992, 1994), www.sox-online.com /coso_cobit. html.

COSO provides that internal control is a system comprising five interrelated elements: internal control environment, risk identification and analysis, control activities (mechanisms), information and communication, and monitoring.

Implementing the COSO concept in the insurance undertaking requires the development of the internal control environment. It should provide a general framework for the other elements of the internal control system (ICS). Elements of the control environment include: top executive's management style; organizational culture of the undertaking; values and ethical standards established, implemented and enforced by the institution, staff competence and their individual features; general attitude to (and awareness of) the executive's control measures, as well as division of responsibilities and powers resulting from the organizational structure.

The institution's executive should ensure correct operation of the ICS and provide all staff members with an appropriate environment for the understanding and proper performance of control tasks. The supervisory board and management board have a special responsibility to promote the control environment as a necessary solution for all organizational levels of the institution. The undertaking's organizational structure should be focused on maintaining professional ethical standards – for example by implementing an appropriate code of ethics or a code of conduct for the institution's staff – and on effective control mechanisms.

Risk identification and analysis should be performed in all areas of the undertaking's operation for which specific targets and implementation criteria were defined, e.g. concerning the sale of insurance policies, marketing and finance, etc. The management board, aware of insurance risks, should institute effective control mechanisms supporting the identification, analysis and management of risks involved in the business activity. Control measures should be adjusted to specific risks to minimize the likelihood of risk occurrence or reduce financial consequences of its occurrence.

In the ICS framework, control measures are a set of provisions and control procedures which are in place to reasonably ensure that the institution's goals are achieved. They comprise: orders; regulations; instructions; procedures; divisions of powers, duties and responsibilities; and the organizational structure. They should be developed for and implemented in all areas in which there are identified risks jeopardizing the achievement of goals. Their aim is to ensure that all activities and measures are implemented in an effective manner. Control activities should be assigned to specific processes and areas within the institution which were previously identified in the process of risk estimation.

Efficient operation of the ICS is determined by free information flow and appropriate communication process. **Information and communications system** is a system of data exchange used within the institution and between the institution and its external environment. The information flow system operates throughout the entire institution. Another key element of the ICS, which also supports information flow processes, is computer systems, particularly integrated systems facilitating the registration and management of insurance

services: both in the undertaking's head office and individual agencies. The systems should be equipped with built-in automatic control mechanisms to ensure that all operations are recorded correctly and efficiently.

Monitoring, the fifth element of the ICS, is a process aimed at verifying whether the remaining element function properly. Monitoring of the effectiveness of the ICS is effected by ongoing review of operations or periodical assessment. Ongoing monitoring is the responsibility of the executive staff in the assigned area of responsibility for particular processes or operations. Periodical assessment is the duty of the internal auditor. Whenever necessary, the ICS should be modified. In this way, the ICS can respond dynamically to changing circumstances or new regulations.

The consecutive Report, COSO II[4], contains eight elements which make up an integrated risk management and internal control system. These are: internal control environment, goal setting, identification of risk factors, risk assessment, preventative measures, control mechanisms and activities, information and communication, and monitoring. The new elements of the concept thus are: goal setting, identification of events and response to risk. Under the new concept, the undertaking should define a set of goals before the executive staff go on to identify risks which may potentially affect goal achievement. Thanks to risk management, the executive staff have goal-setting procedures which refer to the company's mission and vision, and are consistent with the level of risk allowed by the undertaking. Internal and external risk factors which have an impact on goal achievement must be identified and divided into threats and opportunities. Threats and opportunities are then taken into account in the process of setting goals and building the undertaking's strategy. Thanks to response to risk, a new element of the ICS, the executive staff are able to select a proper type of risk reaction, i.e. avoidance, acceptance, reduction or sharing. At a later stage a set of measures are developed to link different risk types to their acceptable level.

IAIS is a standard prepared on the basis of the COSO I and COSO II concepts. The standard recommends insurers to create and implement an integrated risk management system which takes due account of the nature, scale and complexity of the undertaking's business activity and identified risks. Similarly to the COSO standards, it is remarked that the system's structure should be properly integrated with the corporate culture and the specific type of the insurer's business, and – above all – should account for all identifiable risk types. The risk management policy adopted by the executive should define links to capital, qualitative and reporting requirements. The structure of the system must allow for immediate response to changes in the risk profile[5]. IAIS is, however, much narrower in scope than COSO and COSO II.

---

[4] The COSO II Report: Enterprise Risk Management – Integrated Framework, Committee of Sponsoring Organizations of the Treadeway Commision, USA 2004, www.sox-online.com /coso_ cobit. html.

[5] For more details, see Gołąb P., Zintegrowane zarządzanie ryzykiem w przedsiębiorstwach ubezpieczeniowych [in:] Ubezpieczenia non-life, E. Wierzbicka (ed.), CeDeWu, Warsaw 2010.

Role of the audit committee and internal audit in ERM

Insurance undertakings, which are classified as public interest entities, are obliged to establish audit committees (Art. 86 of the Act on Statutory Auditors, 2009). Members of the committee are appointed by the supervisory board from among its members. The committee functions in accordance with regulations approved by the supervisory board. The regulations specify detailed tasks and the course of action in the following areas:

1) supervision of internal control,
2) supervision of financial reports,
3) supervision of risk management,
4) special tasks and powers of the audit committee.

The audit committee oversees the performance of the internal control system. It also evaluates the adequacy of the identification system implemented by the management, monitors risk factors and reduces threats to the undertaking's business. The committee should ensure the effectiveness of internal audit tasks. It should also take steps to safeguard its organizational independence and have access to appropriate sources of information. Other tasks include access to statutory auditors' reports and recommendations.

As part of risk management supervision, the audit committee issues opinions on the following projects:

– principles of prudent and sound management, as well as acceptable risk levels in the undertaking's areas of operation,
– principles governing capital estimation and management,
– the undertaking's key regulations and changes in the regulations.

It also assesses how other functions carry out the procedure of reporting irregularities in the undertaking.

It needs to be stressed that the current Polish law regulating operation of insurance undertakings does not contain any legal provisions or executive regulations detailing the principles of operation of the audit committee and the internal audit system. The Authors believe that the International Standards for the Professional Practice of Internal Audit (2001, 2009), announced by the *Institute of Internal Auditors* (IIA), can be used in the place of missing national legislation. Various Polish financial institutions, following in the footsteps of the public finance sector (which adopted the standards in July 2006), have gradually, and on an individual basis, approved them for application in their business practice.

According to the definition included in the Standards IIA[6], internal audit represents an independent and objective activity aimed at increasing value and improving the organization's operational activity. Internal audit is based on a systematic and structured assessment of a number of processes including risk management, control and corporate governance. Furthermore, it contributes to enhancing their performance. Auditing helps the organiza-

[6] The IIA Standards for the Professional Practice of Internal Auditing, www.iia.org.pl.

tion to achieve its goals by providing assurance that the processes proceed effectively and by advising.

As its basic task, internal audit should focus on efforts to obtain appropriate assurances (perform assessments). An independent and objective assessment of the risk management system, internal control system, processes and operation of organizational units in the insurance undertaking should give the executive staff assurance that they function properly. The auditor's advisory role should contribute to improving the system of business management, particularly in terms of risk management and supervision of the undertaking's business activity.

A number of principles of action laid down in relevant standards support the achievement of internal audit goals. These include: executive staff's responsibility for the internal control system; audit orientation on the improvement of the institution's business operations; high quality of audit; auditors' neutrality, impartiality and objectivity in expressing views; professional attitude, proficiency and due diligence in the auditor's activities; effective utilization of internal audit resources, free flow of information and communication processes specifically[7] and many more. It is important that the undertaking's executive staff, managers and staff from the units being audited do not put any pressures on the auditor. Ensuring the auditor's independence should be the responsibility of the audit committee.

Internal auditing should be performed for all areas of the undertaking's business. It is a management tool used by the company's executive to obtain reasonable assurance that:

1) the institution's aims and tasks are effectively pursued,
2) procedures laid down in legal regulations or adopted by the management board are consistently implemented and followed,
3) the internal control's mechanisms and procedures are adequate and they support correct operation of the institution.

In December 2009 and December 2010 the Sub-Commission for Audit and Internal Control of the Economic and Financial Committee operating at the Polish Insurance Chamber only developed audit programmes for selected processes and areas of insurance enterprises.

Summary

Solvency II, announced in 2009, is universal in nature, applying to all insurance undertakings which carry out insurance activity in the EU. Harmonization of legal regulations will make it easier to conduct insurance business for insurers that are a part of capital groups and international financial conglomerates. Under Solvency II, insurance undertakings in the EU are obliged to undertake broad actions and adopt novel solutions with a view to adjusting their organizational structures and procedures to new capital-related, qualitative and reporting requirements. The Directive contains very important changes which modify the previous approach to risk management, as well as internal and external supervision functions. Pursuant to the Directive, the undertaking's supervisory board, audit

[7] Standards IIA 1100, 1200, 1300, 2130, 2400, 2600.

committee and internal audit are assigned a special role in supervision and internal control. Other key elements include adopted risk management methodologies, particularly the ability to effectively identify, assess and monitor risks, which may guard against significant losses.

It should be stated clearly that the Solvency II Directive only provides very general guidelines. Since there are no detailed legal regulations within that scope, insurers should follow international risk management and internal control standards, as well as international standards regulating internal auditing.

Bibliography

Dyrektywa 2002/87/WE z 16 grudnia 2002 r. w sprawie dodatkowego nadzoru nad instytucjami kredytowymi, zakładami ubezpieczeń oraz przedsiębiorstwami inwestycyjnymi konglomeratu finansowego.

Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Solvency II), Dz. Urz. 335, 17.12.2009.

Gołąb P.: *Zintegrowane zarządzanie ryzykiem w przedsiębiorstwach ubezpieczeniowych*, [w:] *Ubezpieczenia non-life*, red. E. Wierzbicka CeDeWu, Warszawa 2010.

International Associaton of insurance Supervisors: Standard No. 2.2.6. on Enterprise Risk Management for Capital Adequacy and Solvency Purposes, www.iaisweb.org.

The COSO II Report: Enterprise Risk Management – Integrated Framework, Committee of Sponsoring Organizations of the Treadeway Commision, USA 2004, www.sox-online.com /coso_ cobit. html.

The COSO Report: Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadeway Commision, USA (1992, 1994), www.sox-online.com /coso_ cobit. Html.

The International Standards for the Professional Practice of Internal Audit, The Institute of Internal Auditors (IIA), USA, 1998, 2001, 2009, www.iia.org.

Ustawa z 22 maja 2003r. o działalności ubezpieczeniowej, Dz.U. 2010, nr 11, poz. 66.

Ustawa z 7 maja 2009 r. o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym (DzU nr 77, poz. 649).

Dr Maria Kiedrowska
Dr Elżbieta Izabela Szczepankiewicz
Uniwersytet Ekonomiczny w Poznaniu
Katedra Rachunkowości

Summary

EU and national government committees, and financial supervision authorities, have recently undertaken legislative efforts with a view to improving the effectiveness of supervising the business activities pursued by insurance undertakings with a special emphasis on effective risk management and internal control. The culmination of the efforts is the Solvency II Directive. Insurance undertakings operating in the EU are obliged to take broad actions and introduce innovative solutions to adjust their organizational structures and procedures to new capital-related, qualitative and reporting requirements, as laid down in Solvency II.

The article presents the Author's own governance model, comprising integrated risk management and internal control, designed specifically for insurance undertakings, which is based on the Polish laws in place, and Solvency II.

KONTROLA WEWNĘTRZNA W KONCEPCJI ZINTEGROWANEGO SYSTEMU ZARZADZANIA RYZYKIEM (ERM) W ZAKŁADACH UBEZPIECZEŃ

Streszczenie

Obecnie komisje UE, komisje rządowe, instytucje nadzoru finansowego podjęły działania legislacyjne mające na celu zwiększenie efektywności nadzoru nad działalnością zakładów ubezpieczeń, a w szczególności skutecznego zarządzania ryzykiem oraz kontrolą wewnętrzną. Efektem tych prac jest uchwalenie Solvency II. Zakłady ubezpieczeń w krajach UE muszą podjąć bardzo szeroko zakrojone działania i przyjąć nowatorskie rozwiązania w celu dostosowania własnych struktur organizacyjnych i procedur do nowych wymagań kapitałowych, jakościowych i sprawozdawczych, zawartych w Solvency II.

Artykuł prezentuje autorski model systemu zarządzania, obejmujący zintegrowany system zarządzania ryzykiem i kontroli wewnętrznej w zakładach ubezpieczeń, z uwzględnieniem obecnie obowiązujących polskich przepisów prawnych i Solvency II.