Finanse, Rynki Finansowe, Ubezpieczenia nr 4/2018 (94), cz. 1

DOI: 10.18276/frfu.2018.94/1-16 s. 185–195

Model dojrzałości zarządzania ryzykiem i jego aspekty procesowe oraz informatyczne

Wojciech Fliegner*

Streszczenie: *Cel* – Celem artykułu jest zaprezentowanie modelu dojrzałości zarządzania ryzykiem oraz jego aspektów procesowych i na tym tle scharakteryzowanie zakresu wsparcia tego modelu przez technologie informatyczne.
Metodologia badania – Studia literaturowe, obserwacje praktyki gospodarczej, metoda dedukcji.
Wynik – Prezentacja procesowych i informatycznych aspektów dojrzałości zarządzania ryzykiem.
Oryginalność/wartość – Opracowanie narzędzia diagnozującego gotowość organizacji do wykorzystania mniej lub bardziej zaawansowanych rozwiązań informatycznych wspomagających zarządzanie ryzykiem.

Słowa kluczowe: dojrzałość zarządzania ryzykiem, podejście procesowe, technologie informatyczne

Wprowadzenie

Ryzyko towarzyszy każdemu procesowi realizowanemu w organizacji. Jego niezrozumienie, błędna identyfikacja czynników ryzyka czy niewłaściwe zarządzanie nim mogą doprowadzić do utraty możliwości osiągania przez firmy strategicznych celów. Współczesne zarządzanie procesami może być wspomagane przez technologie informatyczne, które ułatwiają modelowanie i wykonanie procesów oraz zapewniają monitorowanie i nadzór nad działaniami procesowymi, umożliwiając w ten sposób usprawnianie procesów. Modele dojrzałości opisują ewolucyjną ścieżkę rozwoju organizacji, wspomagając jej przejście od stanu niespójnych, doraźnych działań związanych z ryzykiem organizacyjnym do działań uporządkowanych, monitorowanych i zarządzanych.

Celem niniejszego artykułu jest – po przedstawieniu istoty zarządzania ryzykiem i wybranych jego standardów – zaprezentowanie modelu dojrzałości zarządzania ryzykiem oraz jego aspektów procesowych i na tym tle scharakteryzowanie zakresu wsparcia tego modelu przez technologie informatyczne, w tym przez rozwiązania nowatorskie rozwijane przez autora artykułu.

* dr hab. Wojciech Fliegner prof. UEP, Uniwersytet Ekonomiczny w Poznaniu, Katedra Rachunkowości, e-mail: wojciech.fliegner@ue.poznan.pl.

1. Istota zarządzania ryzykiem na poziomie organizacji

Pojęcie zarządzania ryzykiem jest definiowane w publikacjach naukowych oraz w dokumentach opisujących standardy w zakresie zarządzania ryzykiem. Na przykład Jajuga definiuje zarządzanie ryzykiem podmiotu jako „podejmowanie decyzji i realizację działań prowadzących do osiągnięcia przez ten podmiot akceptowalnego poziomu ryzyka" (Jajuga, 2007, s. 15). Organizacje standaryzacyjne proponują następujące definicje zarządzania ryzykiem:

- proces, w ramach którego organizacja w sposób metodyczny rozwiązuje problemy związane z ryzykiem – Federacja Europejskich Stowarzyszeń Zarządzania Ryzykiem (Federation of European Risk Management Associations – FERMA),
- system, którego celem jest: identyfikacja potencjalnych zdarzeń mogących wywrzeć wpływ na przedsiębiorstwo, utrzymywanie ryzyka w ustalonych granicach oraz uzyskanie rozsądnego zapewnienia, że cele przedsiębiorstwa będą realizowane – Komitet Organizacji Sponsorujących Komisję Treadwaya (The Committee of Sponsoring Organizations of the Treadway Commission – COSO),
- proces planowania, organizowania, kierowania, wykonywania i kontroli działań w przedsiębiorstwie, mających na celu maksymalizację wartości dla interesariuszy oraz zmniejszenie ryzyka zdarzeń obniżających wartość – Międzynarodowa Federacja Księgowych (International Federation of Accountants – IFAC).

Zarządzanie ryzykiem to złożony proces, który najogólniej można przedstawić w czterech etapach: identyfikacji ryzyka, pomiaru ryzyka, sterowania ryzykiem oraz monitorowania i kontrolowania ryzyka.

Wiele organizacji zarządza ryzykiem w sposób reaktywny, czyli wówczas, gdy wystąpi sytuacja kryzysowa, bądź skupia się na wybranych łatwo mierzalnych ryzykach. W bardziej zaawansowanych rozwiązaniach poszczególne części składowe organizacji zarządzają ryzykiem za pomocą indywidualnie dobranych narzędzi i aplikacji, nie komunikując się z innymi częściami. To podejście do zarządzania ryzykiem określa się mianem silosowego. W większości opracowań stosuje się koncepcję zintegrowanego zarządzania ryzykiem.

W tabeli 1 przedstawiono różnice między silosowym a zintegrowanym podejściem do zarządzania ryzykiem.

Tabela 1

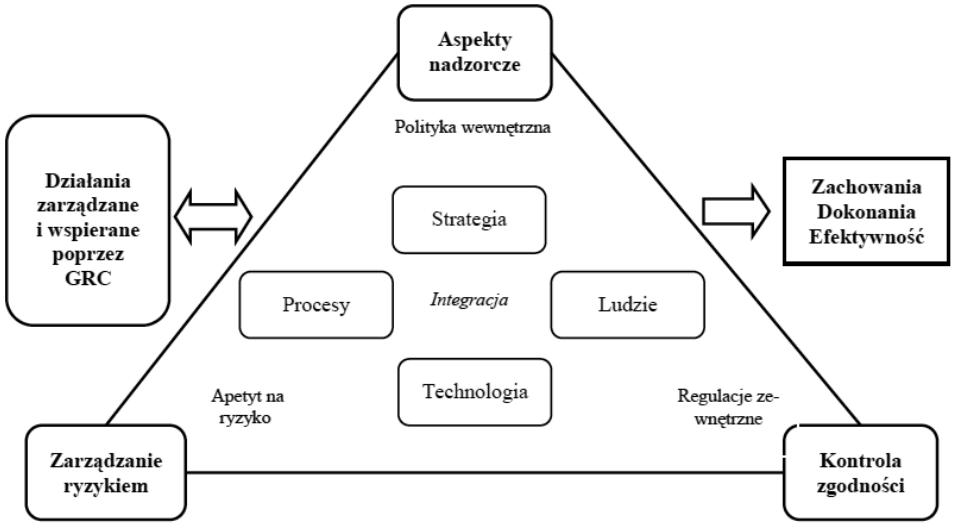
Porównanie cech tradycyjnego i zintegrowanego podejścia do zarządzania ryzykiem

Podejście tradycyjne	Podejście zintegrowane
1	2
Ryzyka rozpatrywane w sposób wyizolowany, tzw. silosowy	Całościowe zarządzanie ryzykiem obejmujące wszystkie występujące w organizacji typy ryzyka
Brak lub znikome powiązanie zarządzania ryzykiem ze strategią firmy	Ścisłe powiązanie zarządzania ryzykiem ze strategią firmy
Niechęć do podejmowania ryzyka	Proaktywna postawa wobec ryzyka

1	2
Sporadyczna ocena ryzyka	Ciągła identyfikacja i ocena ryzyka, weryfikacja i monitoring procesu zarządzania ryzykiem
Ryzyko często nie podlega kwantyfikacji	Większość rodzajów ryzyka podlega kwantyfikacji
Brak lub słaby przepływ informacji, niespójny system raportowania	Dobry przepływ informacji, skonsolidowane raporty
Brak przejrzyście zdefiniowanych ról i zakresów odpowiedzialności	Zdefiniowane role i odpowiedzialność za ryzyko przypisana do procesów biznesowych

Źródło: opracowanie własne na podstawie Banham (2004), s. 65–71.

Podobieństwo wyzwań i uwarunkowań, jakie stoją przed organizacjami chcącymi kontrolować zgodność swoich działań z regulacjami, w kompleksowy sposób zarządzać ryzykiem i wspierać efektywny nadzór nad ich działalnością, zwraca uwagę na możliwość podejścia integrującego wspomniane aspekty (Spanaki, Papazafeiropoulou, 2016; Moeller, 2011). Owa integracja aspektów nadzorczych (*governance*), zarządzania ryzykiem (*risk management*) i kontroli zgodności (*compliance*) oznaczana jest akronimem GRC (rys. 1).



Rysunek 1. Zintegrowane podejście do GRC

Źródło: Racz, Weippl, Seufert (2010), s. 113.

Każda z trzech składowych koncepcji GRC jest kształtowana przez cztery komponenty: strategię, procesy, ludzi i technologię w zależności od akceptowanego poziomu ryzyka, wewnętrznych procedur (polityk) i regulacji zewnętrznych, zaś cele wdrożenia koncepcji definiowane są jako promowanie etycznie poprawnych zachowań oraz poprawa efektywności i skuteczności działań. Takie zintegrowane podejście pozwala uniknąć rozpraszania i duplikowania wysiłków związanych z podejmowanymi w tych obszarach inicjatywami,

a także w większym stopniu uwzględniać interdyscyplinarną naturę ryzyka oraz uzyskać czytelniejszy obraz instytucji, szczególnie w kontekście nadzorczym.

2. Analiza wybranych standardów zarządzania ryzykiem

Wraz z rozwojem zarządzania ryzykiem powstały standardy, które zawierają zbiór najlepszych praktyk oraz pozwalają firmom świadomie i skutecznie wdrażać oraz realizować proces zintegrowanego zarządzania ryzykiem. W tym punkcie zostaną omówione dwa najpopularniejsze standardy: FERMA i COSO[1].

Zgodnie ze standardem FERMA[2] proces zarządzania ryzykiem powinien być realizowany jako sekwencja następujących etapów:

- oceny ryzyka:
  a) analiza, identyfikacja, opis i pomiar ryzyka – dokonanie kompleksowej analizy czynników wewnętrznych i zewnętrznych, określenie rodzajów ryzyka, na jakie jest narażone przedsiębiorstwo, oraz ich prezentacja w czytelnej postaci (np. tabeli) i ocena w sposób ilościowy, półilościowy bądź jakościowy;
  b) ewaluacja ryzyka – wybór rodzajów ryzyka, które w sposób istotny mogą wpływać na sytuację przedsiębiorstwa;
- informowanie o ryzyku oraz o zagrożeniach i szansach z tym związanych,
- działania wobec ryzyka związane z wdrażaniem strategii i instrumentów sterowania ryzykiem,
- raportowanie o ryzyku – dostarczanie informacji różnym pracownikom i komórkom o występującym w organizacji ryzyku i podejmowanych wobec niego działaniach,
- monitorowanie – przeprowadzanie okresowego audytu zasad zarządzania ryzykiem oraz zgodności realizowanego procesu ze standardem, analiza ryzyka ze względu na dynamicznie zmieniające się otoczenie oraz dostarczanie informacji o skuteczności podjętych działań i zastosowanych narzędzi.

W analizowanym standardzie uwzględniono fakt, że ryzyko może się wiązać zarówno z szansami (aspekt pozytywny), jak i zagrożeniami (aspekt negatywny). Celem jego autorów nie było opracowanie normy o charakterze nakazowym, która by wyznaczała precyzyjnie warunki, jakie należy spełnić, czy też stanowiłaby podstawę do wydawania certyfika-

[1] Zagadnienia oceny ryzyka są obecne także w Międzynarodowych Standardach Rewizji Finansowej, opracowanych przez Międzynarodową Federację Księgowych (International Federation of Accountants – IFAC) oraz w Międzynarodowych Standardach Profesjonalnej Praktyki Audytu Wewnętrznego opracowanych przez Międzynarodowy Instytut Audytorów Wewnętrznych (The Institute of Internal Auditors – IIA).

[2] Standard FERMA definiuje pojęcia, procesy służące zarządzaniu ryzykiem, struktury organizacyjne w zarządzaniu ryzykiem oraz cele zarządzania ryzykiem. Standard ten jest promowany przez Federację Europejskich Stowarzyszeń Zarządzania Ryzykiem (FERMA), a został opracowany przez brytyjskie organizacje branżowe: Instytut Zarządzania Ryzykiem (The Institute of Risk Management – IRM), Stowarzyszenie Menedżerów Ubezpieczeniowych i Zarządzających Ryzykiem (The Association of Insurance and Risk Managers – AIRMIC) oraz Krajowe Forum na rzecz Zarządzania Ryzykiem w Sektorze Publicznym – ALARM (ALARM The National Forum for Risk Management in the Public Sector).

tów zgodności – standard FERMA jest w istocie opisem dobrych praktyk o charakterze wzorcowym.

W standardzie COSO[3] zintegrowane zarządzanie ryzykiem zostało opisane jako system – co odróżnia ten standard od standardu FERMA, ujmującego zarządzanie ryzykiem jako proces – złożony z ośmiu powiązanych elementów (komponentów ryzyka). Są to:

1) środowisko wewnętrzne (*Internal Environment*) – obejmuje charakter organizacji, filozofię zarządzania, etykę biznesu, środowisko pracy i akceptowalny poziom ryzyka,
2) ustalanie celów organizacji (*Objective Setting*) zgodnych z jej misją i wizją oraz akceptowanym przez przedsiębiorstwo poziomem ryzyka (*risk appetite*),
3) identyfikacja zdarzeń (*Event Identification*) – dotyczy zdarzeń o zarówno wewnętrznych, jak i zewnętrznych skutkach negatywnych, oznaczających ryzyko, i pozytywnych, stanowiących szanse, oraz ich wpływu na możliwość osiągnięcia celów strategicznych i operacyjnych,
4) ocena ryzyka (*Risk Assesment*) – analiza zakresu, wpływu potencjalnego ryzyka – z podziałem na ryzyko wewnętrzne i nieodłączne – na osiąganie celów,
5) reakcja na wystąpienie ryzyka (*Risk Response*) – wybór metod sterowania ryzykiem przez unikanie, ograniczanie, podział i akceptację ryzyka,
6) działania kontrolne (*Control Activities*) – ustalone procedury realizowane w celu efektywnej reakcji na ryzyko,
7) informacja i komunikowanie się (*Information & Communication*) – zbieranie i przekazywanie informacji potrzebnych do zarządzania ryzykiem i podejmowania merytorycznych decyzji odnośnie do założonych celów,
8) monitorowanie (*Monitoring*) – ocena obecności i funkcjonowania komponentów zarządzania ryzykiem w danym okresie.

Standard COSO wskazuje na bezpośredni związek między celami[4], czyli tym, co organizacja pragnie osiągnąć, a komponentami zarządzania ryzykiem, czyli tym, co jest konieczne do osiągnięcia celów na wszystkich poziomach organizacji. Te trzy perspektywy zintegrowanego zarządzania ryzykiem są ujmowane graficznie w formie trójwymiarowej kostki (COSO Cube), w której cztery kategorie celów są przedstawione w kolumnach, osiem komponentów – w wierszach, a jednostki organizacyjne przedsiębiorstwa – w trzecim wy-

[3] Standard COSO to kompleksowa metodologia, która precyzuje podstawowe pojęcia, zasady i techniki zarządzania ryzykiem oraz kryteria oceny efektywności zintegrowanego systemu zarządzania ryzykiem. Zapisy dotyczące tego standardu, określanego także jako system ERM lub model COSO II, są zawarte w publikacji *Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa* (*Enterprise Risk Management – Integrated Framework*). Pierwszy raport organizacji COSO pt. *Kontrola wewnętrzna – zintegrowana koncepcja ramowa* (*Internal Control – Integrated Framework*), zwany też modelem COSO I, został zaktualizowany i rozszerzony w 2013 roku, rozwijając i jaśniej określając zasady oraz metody zarządzania ryzykiem w kontekście wdrażania i wykorzystywania kontroli wewnętrznej w organizacjach. W modelu COSO II strukturę systemu kontroli wewnętrznej tworzy pięć spośród ośmiu elementów tego modelu – są to: środowisko wewnętrzne, oszacowanie ryzyka, działania kontrolne, informacja i komunikacja oraz monitoring.

[4] Struktura ramowa zarządzania ryzykiem opisana w standardzie COSO koncentruje się na osiąganiu celów przedsiębiorstwa w czterech kategoriach: strategiczne (*strategic*), operacyjne (*operations*), sprawozdawczości (*reporting*) i zgodności z prawem (*compliance*).

miarze. Taka kostka obrazuje zdolność organizacji do objęcia całego zarządzania ryzykiem lub koncentrowania się na kategorii celów, komponencie, jednostce organizacyjnej lub dowolnym ich zbiorze.

Standardy FERMA i COSO mają podobną strukturę. Można dostrzec więcej podobieństw niż różnic między nimi, co świadczy o dążeniu do ujednolicenia zasad, technik i kryteriów.

3. Model dojrzałości zarządzania ryzykiem i jego aspekty procesowe

Zagadnienie dojrzałości organizacji (*organisation's maturity*) pojawiło się w dziedzinie nauk o zarządzaniu w latach 70. XX wieku w kontekście analizy sprawności funkcjonowania firm i instytucji, obok pojęć takich, jak efektywność i skuteczność. Analiza doniesień literaturowych wskazuje, że powstało wiele modeli dojrzałości, wśród których dominującą grupę stanowią modele dojrzałości procesowej i dojrzałości projektowej.

Mimo dużej popularności tego podejścia, dopiero w 2009 roku pojawiła się formalna definicja modelu dojrzałości wskazująca, że prezentuje on „ilościowo lub jakościowo etapy rosnącej zdolności elementów modelu do wykonania stawianych zadań w celu ich oceny w odniesieniu do zdefiniowanych obszarów" (Kohlegger, Maier, Thalmann, 2009, s. 59). Modele dojrzałości opisują zatem sekwencje kolejnych poziomów (stopni) dojrzałości, obrazując pożądaną lub logiczną ścieżkę przechodzenia od stanu początkowego do pełnej dojrzałości, najczęściej od całkowitej niedojrzałości, charakteryzowanej jako doraźność, brak zorganizowania i chaos (poziom 1), przez powtarzalność (poziom 2), standaryzację (poziom 3), świadome zarządzanie (poziom 4), aż po ciągłe usprawnianie i doskonalenie, jako wyraz najwyższej dojrzałości (poziom 5).

Modele dojrzałości mogą realizować trzy funkcje (por. Pöppelbuß, Röglinger, 2011; Maier, Moultrie, Clarkson, 2012):

- funkcję deskryptywną, która pomaga w ustaleniu rzeczywistego poziomu dojrzałości organizacji, w danym momencie,
- funkcję preskryptywną, która opisuje pożądany stan docelowy i określa lukę występującą między stanem istniejącym a stanem pożądanym,
- funkcję definiującą zakres przejścia, która wskazuje, jakie działania należy wykonać, aby od stanu istniejącego przejść do pożądanego.

Na podstawie literatury przedmiotu, obserwacji praktyki biznesowej oraz badań własnych proponuje się wyróżnienie następujących poziomów dojrzałości organizacji w zakresie zarządzania ryzykiem:

- poziom 1 (*inicjacja zarządzania ryzykiem*) – działania związane z zarządzaniem ryzykiem są realizowane w sposób improwizowany; strategia reaktywna, czyli działania *ad hoc* są podstawowym sposobem działania w przypadku materializacji ryzyka,
- poziom 2 (*procedury zarządzania ryzykiem*) – lokalne (ograniczone do wybranych działów) procedury zarządzania ryzykiem oraz związane z nimi role i odpowiedzialności,

- poziom 3 (*standardy organizacyjne*) – organizacja ma zdefiniowane procedury zarządzania ryzykiem na poziomie organizacji, czyli standardy planowania i obsługi ryzyka z wykorzystaniem mierników oceny i nadaniem priorytetów określonym rodzajom ryzyka są stosowane na każdym poziomie zarządzania organizacją,
- poziom 4 (*zarządzanie procesem*) – w organizacji zostały opracowane sposoby pomiaru i monitorowania jakości oraz efektywności zdefiniowanych standardów zarządzania ryzykiem,
- poziom 5 (*ciągłe usprawnianie procesów*) – organizację, jak i jej procesy charakteryzuje wysoki poziom innowacyjności w zakresie procedur zarządzania ryzykiem; działania w obszarze zarządzania ryzykiem podlegają nieustannej analizie i doskonaleniu (modyfikacji).

Można wskazać następujące, związane z perspektywą procesową, uwarunkowania przejścia między kolejnymi poziomami proponowanego modelu dojrzałości zarządzania ryzykiem:

- poziom 1 → poziom 2 – świadomość istnienia procesów, dokumentowanie i zrozumienie ich struktury,
- poziom 2 → poziom 3 – ustalenie metryk procesu, pomiar procesu i wdrożenie systemu zarządzania procesem, pojawienie się właścicieli procesu (ogólniej nadanie ról procesowych pracownikom),
- poziom 3 → poziomy 4 i 5 – zarządzanie skupione na procesach (orientacja procesowa).

Przełomowy jest trzeci poziom dojrzałości, na którym w zarządzaniu ryzykiem następuje przejście organizacji od podejścia funkcjonalnego (silosowego) w kierunku podejścia procesowego.

4. Informatyczne wspomaganie zarządzania ryzykiem

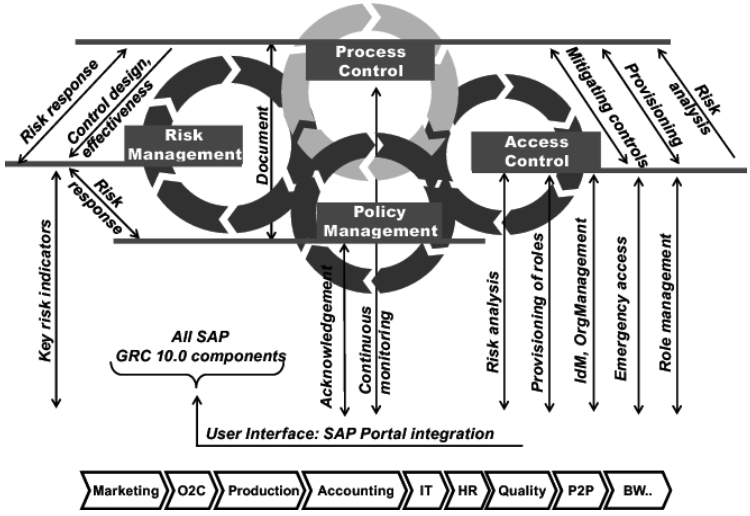
Wykorzystanie technologii informatycznych jest jednym z kluczowych czynników udanego wdrożenia systemu i procesu zarządzania ryzykiem[5] w przedsiębiorstwie. Co więcej, gotowość organizacji do sięgania po coraz bardziej zaawansowane technologicznie rozwiązania informatyczne umożliwia organizacji – po spełnieniu także odpowiednich wymagań proceduralnych, organizacyjnych i kadrowych – osiąganie scharakteryzowanych wcześniej kolejnych poziomów dojrzałości zarządzania ryzykiem.

Na potrzeby niniejszego artykułu proponuje się podział analizowanych rozwiązań informatycznych na podstawowe i zaawansowane, przy czym na poziomach 2. i 3. modelu dojrzałości wystarcza informatyczne wsparcie zarządzania ryzykiem w wariancie określonym tu jako podstawowy, a na poziomach 4. i 5. wymagany jest wariant zaawansowany.

[5] System zarządzania ryzykiem jest tu rozumiany jako zbiór powiązanych ze sobą elementów, którego zadaniem jest zarządzanie ryzykiem. Tworzą go osoby bezpośrednio zaangażowane do realizacji tego zadania, narzędzia IT, rozwiązania organizacyjne, zasoby informacyjne, struktury decyzyjne itp. Proces zarządzania ryzykiem to sekwencja działań mających na celu osiągnięcie wcześniej zdefiniowanego i zaplanowanego rezultatu.

W ujęciu bardziej szczegółowym zakres możliwości informatycznego wsparcia procesów zarządzania ryzykiem zostanie zaprezentowany przez odniesienie istniejących narzędzi informatycznych do struktury ramowej, jaką jest związana ze standardem COSO trójwymiarowa kostka COSO Cube.

W pierwszej kolejności należy przyjrzeć się rozwiązaniom związanym z zarządzaniem ryzykiem usytuowanym w zintegrowanych systemach informatycznych klasy ERP i CRM, przeznaczonych do wspomagania ogółu procesów biznesowych organizacji. Punktem odniesienia uczyniono system SAP. W systemie tym wspomaganie zarządzania ryzykiem jest realizowane w ramach koncepcji GRC, o której wspomniano w pierwszym punkcie niniejszego artykułu, za pośrednictwem czterech modułów (zob. rys. 2): SAP GRC Access Control, SAP GRC Process Control, SAP Risk Management i SAP Policy Management[6]. Jak wynika z rysunku 2, rozwiązanie to wspiera komponenty ryzyka wyspecyfikowane w standardzie COSO jako pozycje 4–8 (zob. punkt drugi niniejszego artykułu).



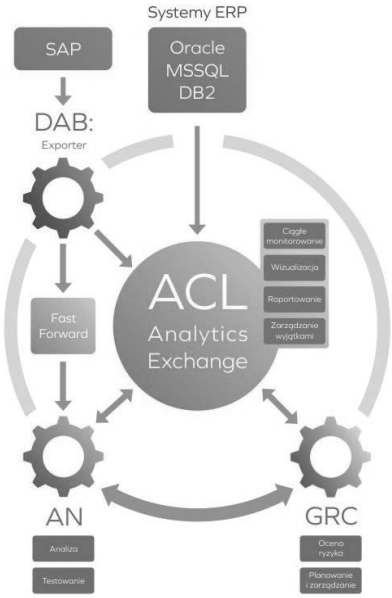
Rysunek 2. Realizacja koncepcji GRC w systemie SAP

Źródło: Chuprunov (2013), s. 80.

Analiza aktualnej oferty oprogramowania umożliwia przedstawienie bardziej uniwersalnej propozycji kompleksowego wsparcia zarządzania ryzykiem. Zestaw ten tworzy pięć elementów składowych (zob. rys. 3) pochodzących od dwóch dostawców[7].

[6] Do wsparcia realizacji aspektów nadzorczych (*governance*) przeznaczony jest moduł Policy Management; zarządzanie ryzykiem odbywa się poprzez moduły Access Control i Risk Management, a kontrola zgodności (*compliance*) opiera się na module Process Control. Wersję podstawową rozwiązania SAP stanowi moduł Access Control.

[7] Są to firmy: ACL (http://www.acl.com) i DAB (http://www.dab-europe.com).



Rysunek 3. Propozycja kompleksowego wsparcia zarządzania ryzykiem
Źródło: opracowanie własne.

Rodzina produktów firmy ACL obejmuje trzy rozwiązania, które w obszarach *governance*, zarządzania ryzykiem i kontroli zgodności mogłyby wspierać identyfikację, badanie i ograniczanie ryzyka biznesowego. Owo wsparcie obejmowałoby[8]:

– w wariancie podstawowym: analizę danych (za pomocą modułu ACL Analytics) w celu wykrycia nieprawidłowych transakcji z perspektywy norm biznesowych, standardów kontroli wewnętrznej lub wymagań prawnych oraz ciągłe monitorowanie kluczowych obszarów funkcjonowania firmy za pomocą modułu ACL Enterprise Continuous Monitoring (ECM), uzupełnionego o technologię ACL Analytics Exchange[9], jako systemu wczesnego ostrzegania o ryzyku,
– w wariancie zaawansowanym: integrację działań w zakresie nadzoru (*governance*), zarządzania ryzykiem (*risk management*) i kontroli zgodności (*compliance*) za pomocą modułu ACL GRC.

[8] Przedstawioną tu propozycję uzupełniają dwa rozwiązania związane ze środowiskiem systemów zintegrowanych klasy ERP – działałyby one w dwóch obszarach: ekstrakcji i pobierania danych z systemu zintegrowanego (moduł dab:Exporter) oraz analizy danych z wykorzystaniem predefiniowanych testów analitycznych (moduł dab:FastForward).

[9] Autor niniejszego artykułu realizuje prace projektowo-programistyczne mające na celu rozbudowę funkcjonalności tego segmentu analizowanej tu propozycji. Działania te można usytuować w obszarze badań określanych mianem odkrywania procesów (*process mining*); koncentrują się one na monitorowaniu przebiegu procesów biznesowych oraz identyfikacji i oceny związanych z nimi rodzajów ryzyka.

W przypadku proponowanego rozwiązania jego wariant podstawowy wspiera komponenty ryzyka wyspecyfikowane w standardzie COSO jako pozycje 6 (działania kontrolne) i 8 (monitorowanie), a wdrożenie wariantu zaawansowanego rozszerza to wsparcie na komponenty z pozycji 4, 5 i 7 (zob. punkt drugi niniejszego artykułu).

Uwagi końcowe

Zarządzanie ryzykiem polega na identyfikacji i kontrolowaniu – przez neutralizowanie zagrożeń i wykorzystywanie szans – tych rodzajów ryzyka, które mogą wpływać na realizację celów strategicznych firmy. Pomocą dla menedżerów we wdrażaniu systemu zarządzania ryzykiem mogą być modele dojrzałości, które podpowiadają drogę postępowania, zwiększającą prawdopodobieństwo sukcesu. W artykule przedstawiono zarys takiego modelu dojrzałości. Model ten – zdaniem autora – może stanowić narzędzie diagnostyczne do oceny gotowości organizacji do wykorzystania mniej lub bardziej zaawansowanych rozwiązań informatycznych wspomagających zarządzanie ryzykiem.

Literatura

Banham, R. (2004). Enterprising Views of Risk Management. *Journal of Accountancy*, *6* (197), 65–71.

Chuprunov, M. (2013). *Auditing and GRC Automation in SAP*. Berlin–Heidelberg: Springer.

Jajuga, K. (2007). Koncepcja ryzyka i proces zarządzania ryzykiem – wprowadzenie. W: *Zarządzanie ryzykiem*, red. K. Jajuga (s. 13–32). Warszawa: Wydawnictwo Naukowe PWN.

Kohlegger, M., Maier, R., Thalmann, S. (2009). Understanding Maturity Models. Results of a Structured Content Analysis. W: *Proceedings of I-KNOW'09 and I-SEMANTICS'09* (s. 51–61). Graz.

Maier, A.M., Moultrie, J., Clarkson, P.J. (2012). Assessing Organizational Capabilities: Reviewing and Guiding the Development of Maturity Grids. *IEEE Transactions on Engineering Management*, *1* (59), 138–159.

Moeller, R.R. (2011). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Process*. Hoboken: Wiley.

Pöppelbuß, J., Röglinger, M. (2011). What Makes a Useful Maturity Model? A Framework of General Design Principles for Maturity Models and its Demonstration in Business Process Management. W: *Proceedings of the Nineteenth European Conference on Information Systems (ECIS 2011)*. Helsinki: Association for Information Systems (AIS).

Racz, N., Weippl, E., Seufert, A. (2010). A Frame of Reference for Research of Integrated Governance, Risk, and Compliance (GRC). W: *Lecture Notes in Computer Science*, *6109* (s. 106–117). Berlin–Heidelberg: Springer.

Spanaki, K., Papazafeiropoulou, A. (2016). The Implementation of Governance, Risk, and Compliance. *Information Systems Management*, *4* (33), 302–315.

MODEL OF RISK MANAGEMENT MATURITY AND ITS PROCESS AND IT ASPECTS

Abstract: *Purpose* – The aim of the article is to present the risk management maturity model and its process aspects and, in this context, to characterize the scope of support of this model through IT technologies.
Design/methodology/approach – Literature studies, observations of business practice, the method of deduction.
Findings – Presentation of process and IT aspects of risk management maturity.

Originality/value – Development of a tool that diagnoses the organization's readiness to use more or less advanced IT solutions supporting risk management.

Keywords: risk management maturity, process approach, IT technologies

Cytowanie
Fliegner, W. (2018). Model dojrzałości zarządzania ryzykiem i jego aspekty procesowe oraz informatyczne. *Finanse, Rynki Finansowe, Ubezpieczenia*, *4* (94/1), 185–195. DOI: 10.18276/frfu.2018.94/1-16.