



Wojciech Fliegner

Uniwersytet Ekonomiczny w Poznaniu
Wydział Zarządzania
Katedra Rachunkowości
wojciech.fliegner@ue.poznan.pl

INFORMATYCZNE ASPEKTY PODEJŚCIA PROCESOWEGO JAKO SKŁADOWEJ MODELU DOJRZAŁOŚCI ZARZĄDZANIA RYZYKIEM W ORGANIZACJI

Streszczenie: Celem niniejszego artykułu jest – po przedstawieniu istoty zarządzania ryzykiem i roli audytu w procesie zarządzania ryzykiem – zaprezentowanie modelu dojrzałości zarządzania ryzykiem oraz jego aspektów procesowych i na tym tle scharakteryzowanie zakresu wsparcia tego modelu przez technologie informatyczne wykorzystywane w ramach audytu, w tym przez rozwiązania nowatorskie rozwijane przez autora artykułu.

Słowa kluczowe: zarządzanie ryzykiem, model dojrzałości, podejście procesowe.

Wprowadzenie

Ryzyko towarzyszy każdemu procesowi realizowanemu w organizacji. Jego niezrozumienie, błędna identyfikacja czynników ryzyka czy niewłaściwe zarządzanie nim mogą doprowadzić do utraty możliwości osiągnięcia 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 ciągłe 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 roli audytu w procesie zarządzania ryzykiem – zaprezentowanie modelu dojrzałości zarządzania ryzykiem oraz jego aspektów procesowych i na tym tle scharakteryzowanie zakresu wsparcia tego modelu przez technologie informatyczne wykorzystywane w ramach audytu, w tym przez rozwiązania nowatorskie rozwijane przez autora artykułu.

1. Istota zarządzania ryzykiem na poziomie organizacji

Zarządzanie ryzykiem na poziomie przedsiębiorstwa jest definiowane w publikacjach naukowych oraz w dokumentach opisujących standardy w zakresie zarządzania ryzykiem. Definicje te prezentują różnorodność interpretacji tego pojęcia: od rozumienia bardzo wąskiego – technicznego – po rozumienie holistyczne.

Dla przykładu warto przywołać kilka propozycji definiowania pojęcia zarządzania ryzykiem sformułowanych przez organizacje standaryzacyjne:

- 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);
- proces, którego celem jest: identyfikacja potencjalnych zdarzeń mogących wywrzeć wpływ na przedsiębiorstwo, utrzymywanie ryzyka w granicach oraz rozsądne zapewnienie realizacji celów przedsiębiorstwa – Komitet Organizacji Sponsorujących Komisję Treadwaya (The Committee of Sponsoring Organizations of the Treadway Commission, COSO);
- proces identyfikacji, oceny, kierowania i kontroli potencjalnych zdarzeń oraz sytuacji, zmierzający do dostarczenia racjonalnego zapewnienia, że cele organizacji (przedsiębiorstwa) zostaną zrealizowane – Międzynarodowy Instytut Audytorów Wewnętrznych (The Institute of Internal Auditors, IIA);
- 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).

W literaturze przedstawia się zarządzanie ryzykiem m.in. jako ciąg działań skierowanych na ograniczanie wpływu na organizację nieprzewidywalnych czynników zewnętrznych i wewnętrznych poprzez:

- systematyczne badanie problemu ryzyka w całości organizacji, czyli analizę zewnętrznych, losowych czynników oraz innych zagrożeń generowanych przez samą organizację;

- szacowanie poziomu ryzyka jako prawdopodobieństwa wystąpienia poszczególnych zagrożeń oraz poszukiwanie związków synergicznych między poszczególnymi ryzykami;
- implementację kompleksowej strategii reakcji na ryzyko.

Wiele organizacji zarządza ryzykiem w sposób reaktywny, czyli wówczas, gdy wystąpi sytuacja kryzysowa bądź skupia na wybranych, łatwo mierzalnych ryzykach. W bardziej zaawansowanych rozwiązaniach poszczególne pionory organizacji zarządzają ryzykiem za pomocą własnych narzędzi i aplikacji, nie komunikując się z innymi pionami (to podejście do zarządzania ryzykiem określa się mianem silosowego). Większość opracowań sugeruje realizację koncepcji zintegrowanego zarządzania ryzykiem (*enterprise risk management, ERM*)¹.

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

Tabela 1. Porównanie cech tradycyjnego i zintegrowanego podejścia do zarządzania ryzykiem

Podejście tradycyjne	Podejście zintegrowane
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
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 przejrzystości zdefiniowanych ról i zakresów odpowiedzialności	Zdefiniowane role i odpowiedzialność za ryzyko przypisana do procesów biznesowych

Źródło: Na podstawie Banham [2004, s. 65-71].

2. Audyt jako preferowana metoda zarządzania ryzykiem i jego kontekst procesowy

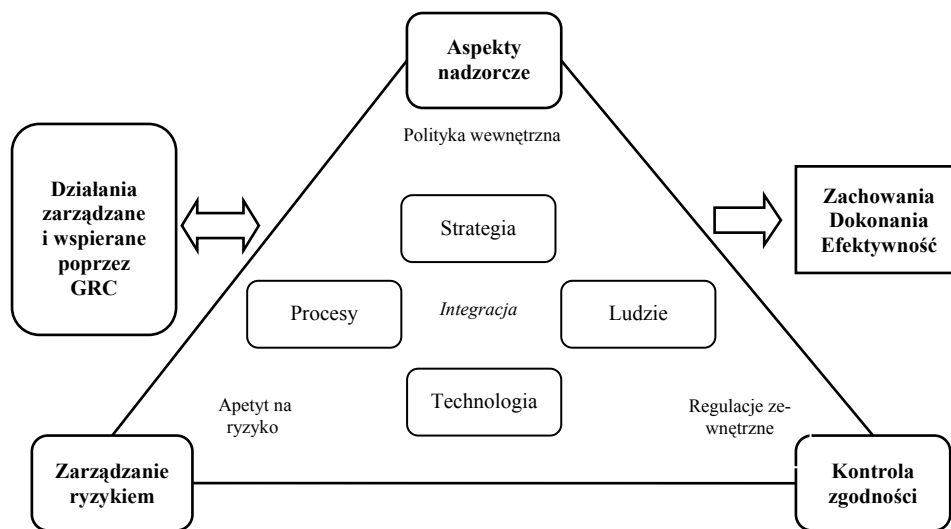
Definicja audytu wewnętrznego – opracowana przez The Institute of Internal Auditors (IIA)² – wskazuje, że audyt wewnętrzny powinien wspierać organizacje w osiąganiu wytyczonych celów poprzez systematyczne działania służące

¹ Warto tu odnotować istnienie zbieżnego z tą koncepcją modelu zatytułowanego *Enterprise Risk Management Integrated Framework*, zaprezentowanego przez wspomnianą wyżej organizację standaryzacyjną COSO w raporcie z 2004 r. Model ten wskazuje osiem elementów tworzących zintegrowany system zarządzania ryzykiem, wiążąc je z czterema kategoriami celów przedsiębiorstwa na czterech poziomach jego funkcjonowania.

² Jest to największa międzynarodowa organizacja zrzeszająca audytorów wewnętrznych.

ocenie i poprawie skuteczności procesów zarządzania ryzykiem oraz – pozostające poza obszarem niniejszych rozważań – działania dotyczące systemu kontroli i ładu organizacyjnego (*governance*) [International..., 2001, s. 3].

Podobieństwo wyzwań i uwarunkowań, jakie stoją przed instytucjami chcącymi kontrolować zgodność z regulacjami, w kompleksowy sposób zarządzać ryzykiem i wspierać efektywny nadzór nad ich działalnością, zwraca uwagę na możliwość podejścia integrującego wspomniane aspekty [Racz i in., 2010]. Owa integracja aspektów nadzorczych (*governance*), zarządzania ryzykiem (*risk management*) i kontroli zgodności (*compliance*) oznaczana jest akronimem GRC (rys. 1).



Rys. 1. Zintegrowane podejście do GRC

Źródło: Racz i in. [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.

Nowoczesny audyt wewnętrzny realizuje powyższy cel poprzez badanie procesów gospodarczych, w których zidentyfikowano najistotniejsze ryzyka

organizacji. Jego rola związana jest z weryfikacją procedur kontrolnych w odniesieniu do tych procesów. W trakcie planowania prac działań audytorskich możliwe są dwa sposoby postępowania:

- można dokonać przypisania procesów do każdego z istotnych dla organizacji rodzajów ryzyka i dokonywać audytu wszystkich procesów, w których to ryzyko występuje;
- można dokonać przypisania istotnych dla organizacji rodzajów ryzyka do każdego z wyróżnionych procesów i dokonywać audytu danego procesu pod kątem wystąpienia w nim różnych (istotnych) rodzajów ryzyka.

Podejście procesowe oraz możliwość wykorzystania technologii informatycznych we wdrożeniach systemów zarządzania ryzykiem wymusiły zmiany w postrzeganiu audytu jako metody zarządzania ryzykiem. W warstwie pojęciowej spowodowało to pojawienie się pojęcia ciągłego audytu (*continuous audit*)³.

3. Proponowany 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 w. w kontekście analizy sprawności funkcjonowania firm i instytucji⁴. Za pierwszy model dojrzałości jest uznawana macierz dojrzałości zarządzania jakością (*Quality Management Maturity Grid*) [zob. Crosby, 1979]. W następnych latach opracowano modele dojrzałości dla innych obszarów zarządzania. Wśród nich dominującą grupę stanowią modele dojrzałości procesowej⁵ i dojrzałości projektowej⁶.

³ Chan i Vasarhelyi [2011] wyróżnili (oraz przeanalizowali w konfrontacji z tradycyjnym audytem) siedem następujących wymiarów innowacyjności idei ciągłego audytu: częstotliwość (cykliczność) audytu, proaktywność modelu audytu, stopień automatyzacji procedur audytu, treść ról audytorów wewnętrznych i zewnętrznych, istotę, zakres i wymiar czasowy testów audytorskich, techniki modelowania i analizy danych, raportowanie wyników audytu. Zob. także [Fliegner, 2015a].

⁴ Uprzednio w analizie tego aspektu funkcjonowania organizacji wykorzystywano najczęściej takie pojęcia jak efektywność (rozumianą jako stosunek osiągniętych korzyści do poniesionych nakładów) i skuteczność (czyli stopień, w jakim dane działanie spełnia postawione przed nim cele) – por. [Głuszek, 2014].

⁵ Dojrzałość procesowa jest stopniowalna (może być niższa lub wyższa) i oznacza zdolność organizacji do efektywnego zarządzania procesami, czyli umiejętność definiowania, pomiaru, zarządzania ilościowego i ciągłego udoskonalania procesu – powstała tu cała rodzina modeli CMM, którą w 2001 r. zintegrowano w jeden ogólniejszy model CMMI (*Capability Maturity Model Integrated*) – zob. [Kania, 2013].

⁶ Analiza doniesień literaturowych wskazuje, że powstało kilkadziesiąt tego typu modeli – zob. [Juchniewicz, 2009].

Obecnie zastosowanie modeli dojrzałości jest bardzo szerokie, obejmuje obszary od organizacji badań naukowych po zastosowania biznesowe i inżynierskie. Mimo tak dużej popularności tego podejścia dopiero w 2009 r. Kohlegger, Maier i Thalmann sformułowali formalną definicję modelu dojrzałości wskazując, 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 i in., 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 dorażność, brak zorganizowania i chaos (poziom 1), przez powtarzalność (poziom 2), standaryzację (poziom 3), świadome zarządzanie (poziom 4), aż po ciągle usprawnianie i doskonalenie jako wyraz najwyższej dojrzałości (poziom 5).

Modele dojrzałości mogą realizować trzy funkcje [por. Röglinger i Pöppelbuß, 2011; Maier i in., 2012]:

- funkcję deskryptywną, która pomaga w ustaleniu, jaki jest w danym momencie rzeczywisty poziom dojrzałości organizacji;
- funkcję preskryptywną, która opisuje pożądaný stan docelowy i określa lukę, jaka występuje pomiędzy stanem istniejącym a stanem pożądanym;
- funkcję definiującą zakres przejścia, która mówi, jakie działania należy wykonać, aby od stanu istniejącego przejść do pożądanego.

W literaturze udokumentowano istnienie kilku modeli dojrzałości zarządzania ryzykiem na poziomie organizacji – są to:

- model Hillsona [Hillson, 1997], który tworzą cztery poziomy dojrzałości (naiwny, debiutancki, znormalizowany, naturalny) powiązane z czterema atrybutami/wymiarami (kultura, procesy, doświadczenie, stosowalność);
- model Hopkinsona [Chapman, 2006], który obejmuje cztery poziomy dojrzałości (o nazwach identycznych jak w modelu Hillsona) i sześć atrybutów (zarządzanie, identyfikacja ryzyka, analiza ryzyka, sterowanie ryzykiem, przegląd ryzyka, kultura);
- model RIMS RMM [Farrell i Gallagher, 2014] z pięcioma poziomami dojrzałości (*ad hoc*, inicjalny, powtarzalny, zarządzany, przywództwo) i siedmioma atrybutami (adaptacja podejścia ERM, zarządzanie procesami ERM, zarządzanie apetytem na ryzyko, docieranie do przyczyn, identyfikacja ryzyka, zarządzanie efektywnością, odporność i trwałość biznesu);
- model AON (*AON's Risk Maturity Index*) [Global, 2010], który identyfikuje pięć poziomów dojrzałości (inicjalny, podstawowy, definiowania, operacyjny, zaawansowany) powiązanych z dziewięcioma atrybutami/wymiarami

(zaangażowanie zarządu w ERM, skłonność do ryzyka, kultura zarządzania ryzykiem, zaangażowanie interesariuszy, komunikacja ryzyka, decyzyjny kontekst ryzyka, uwzględnienie metod ilościowych, identyfikacja ryzyka, kontekst szans związanych z ryzykiem).

Na podstawie literatury przedmiotu, obserwacji praktyki biznesowej oraz badań własnych proponujemy 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 zwykle do działów) procedury zarządzania ryzykiem oraz związane z nimi role i odpowiedzialności;
- poziom 3 (*standardy organizacyjne*) – organizacja posiada zdefiniowane procedury zarządzania ryzykiem na poziomie organizacji; standardy planowania i obsługi ryzyka z wykorzystaniem mierników oceny i priorytetyzacji ryzyka są wykorzystywane na każdym poziomie organizacyjnym;
- poziom 4 (*zarządzanie procesem*) – opracowane zostały 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.

Można wskazać następujące, związane z perspektywą procesową, uwarunkowania przejścia między kolejnymi poziomami proponowanego wyżej 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 → poziom 4 i 5 – zarządzanie skupione na procesach (orientacja procesowa).

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

Przywołane poziomy dojrzałości mogą zdaniem autora stanowić narzędzie diagnostyczne, służące do ustalenia gotowości organizacji do wykorzystania mniej lub bardziej zaawansowanych rozwiązań informatycznych wspomagających – poprzez procedury audytu – zarządzanie ryzykiem na poziomie przedsiębiorstwa⁷.

4. Podejście procesowe w funkcjonowaniu komputerowego wspomaganie zarządzania ryzykiem

Analiza aktualnej oferty oprogramowania umożliwia przedstawienie poniższej propozycji kompleksowego wsparcia ciągłego audytu. Zestaw ten tworzy pięć elementów składowych pochodzących od dwóch dostawców⁸ (rys. 2).

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

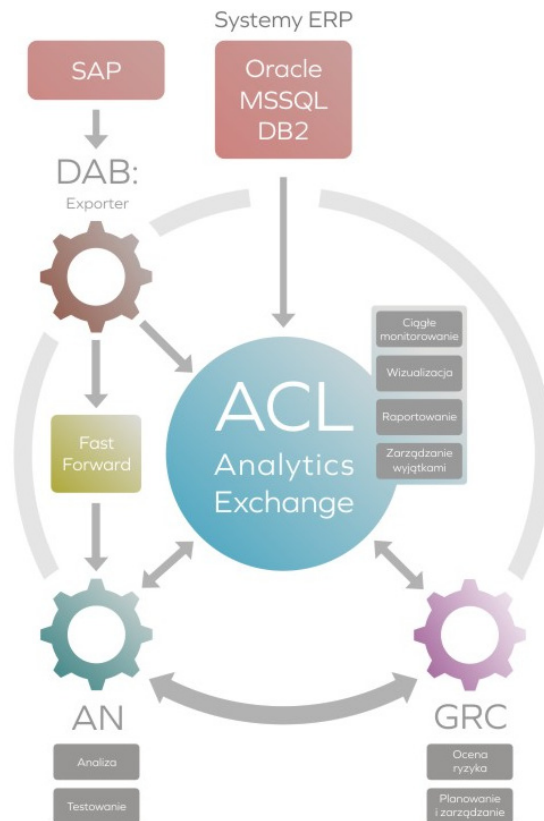
- analizę danych (za pomocą modułu ACL Analytics) – analiza *ad hoc* populacji danych miałyby na celu wykrycie – z perspektywy norm biznesowych, standardów kontroli wewnętrznej i/lub wymogów prawnych – nieprawidłowych transakcji;
- ciągłe monitorowanie kluczowych obszarów (za pomocą modułu ACL Enterprise Continuous Monitoring (ECM) uzupełnionego o technologię ACL Analytics Exchange) – cykliczne analizy danych transakcyjnych pełniłyby rolę systemu wczesnego ostrzegania w celu zapobiegania i łagodzenia skutków biznesowych wynikających ze zidentyfikowanych operacyjnych braków lub luk;
- integrację inicjatyw w obszarze GRC (za pomocą modułu ACL GRC) – zarządzanie i pomiar ryzyka oraz wydolności mechanizmów kontrolnych w stosunku do celów biznesowych zgodnie z przyjętymi przepisami, normami, politykami i decyzjami biznesowymi.

Przedstawioną tu propozycję uzupełniają dwa rozwiązania łączące się z realizacją ciągłego audytu w środowisku systemów zintegrowanych klasy ERP. Działałyby one na dwóch płaszczyznach:

- ekstrakcji i pobierania danych z systemu zintegrowanego (moduł *dab:Exporter*);
- analizy danych z wykorzystaniem predefiniowanych testów analitycznych (moduł *dab:FastForward*).

⁷ Zob. [Fliegner, 2015b]. Na poziomach 2 i 3 wystarczające jest informatyczne wsparcie zarządzania ryzykiem poprzez procedury audytu w wariantcie określonym (w tymże artykule) jako podstawowy, a na poziomach 4 i 5 w wariantcie zaawansowanym (m.in. z wykorzystaniem systemu GRC).

⁸ Są to firmy: ACL (<http://www.acl.com>) i DAB (<http://www.dab-europe.com>).



Rys. 2. Propozycja kompleksowego wsparcia ciągłego audytu

Autor niniejszego artykułu realizuje prace mające na celu rozbudowę funkcjonalności proponowanego rozwiązania. Działania te można usytuować w obszarze badań określanym mianem odkrywania procesów (*process mining*), który koncentruje się na metodach i narzędziach wykorzystywanych do budowy modeli procesów, ich weryfikacji i rozbudowy [Process, 2012] na podstawie danych pochodzących z dzienników zdarzeń powszechnie dostępnych we współczesnych systemach informatycznych⁹, gdzie dane te opisują rzeczywisty (tj. niehipotetycz-

⁹ Są to m.in. systemy zarządzania przepływem prac (Workflow Management Systems, WfMS), systemy ERP (Enterprise Resource Planning) i systemy CRM (Customer Relationship Management). Systemy te rejestrują wiele szczegółowych danych o realizowanych czynnościach (działaniach) i zdarzeniach procesowych. Zbiory takich danych określa się mianem dzienników zdarzeń (*event logs*). Są one punktem wyjścia do eksploracji procesów – wszystkie metody odkrywania procesów zakładają, że możliwy jest sekwencyjny zapis owych zdarzeń w taki sposób, żeby każde zdarzenie odpowiadało czynności wykonanej w procesie i było powiązane z konkretną instancją procesu.

ny) przebieg procesów biznesowych. Aby zaprezentować możliwość wykorzystania proponowanej metody, zrealizowano procedurę ekstrakcji danych procesowych i przedstawiono w innych artykułach autora [por. np. Fliegner, 2014] rezultaty analizy charakterystyk procesów stanowiących kontekst badanych przypadków.

Badania te odwołują się do koncepcji GRC zakładającej konieczność wspólnego i jednolitego podejścia do: zrozumienia (identyfikacji i opisu) działania procesów w instytucji, monitorowania ich realizacji oraz identyfikacji i oceny związanych z nimi rodzajów ryzyka (zob. rys. 1). Jednym z podstawowych wyzwań związanych z wdrażaniem zintegrowanego podejścia GRC jest dopasowanie już funkcjonujących procesów i rozwiązań do wymagań narzuconych przez to podejście.

Podsumowanie

Zarządzanie ryzykiem, czyli niepewnością związaną ze zdarzeniami, zagadnieniami lub działaniami (wewnątrz lub z zewnątrz firmy), które mogą wzmocnić lub zniszczyć zaufanie interesariuszy, wydaje się koniecznością. Polega ono na identyfikacji i kontrolowaniu tych wszystkich rodzajów ryzyka, które mogą wpływać na realizację celów strategicznych firmy – neutralizując zagrożenia i wzmacniając szanse. Pomocą dla menedżerów we wdrażaniu systemu zarządzania ryzykiem mogą być modele dojrzałości, które podpowiadają pewną drogę postępowania zwiększającą prawdopodobieństwo sukcesu. W artykule przedstawiono zarys takiego modelu dojrzałości. Model ten może zdaniem autora stanowić narzędzie diagnostyczne, służące do ustalenia gotowości organizacji do wykorzystania mniej lub bardziej zaawansowanych rozwiązań informatycznych wspomagających – poprzez procedury audytu – zarządzanie ryzykiem na poziomie przedsiębiorstwa.

Literatura

Banham R. (2004), *Enterprising Views of Risk Management*, „Journal of Accountancy”, Vol. 197(6).

Chan D.Y., Vasarhelyi M.A. (2011), *Innovation and practice of continuous auditing*, „International Journal of Accounting Information Systems”, Vol. 12(2).

Chapman R.J. (2006), *Simple Tools and Techniques for Enterprise Risk Management*, Wiley, Chichester.

Crosby P. (1979), *Quality is free*, McGraw Hill, New York.

- Farrell M., Gallagher R. (2014), *The Valuation Implications of Enterprise Risk Management Maturity*, „The Journal of Risk and Insurance”, March.
- Fliegner W. (2015a), *Koncepcja ciągłego audytu i jej informatyczne wsparcie* [w:] M. Remlein (red.), *Rachunkowość warta poznania. Teoria, praktyka, polityka rachunkowości*, Uniwersytet Ekonomiczny w Poznaniu.
- Fliegner W. (2015b), *Informatyczne wspomaganie zarządzania ryzykiem poprzez procedury audytu*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 399.
- Fliegner W. (2014), *Metoda identyfikacji procesów ewidencji księgowej w środowisku informatycznym*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 344.
- Global Enterprise Risk Management Survey 2010* (2010), AON Corporation, Chicago, January.
- Głuszek E. (2014), *Zarys modelu dojrzałości zarządzania ryzykiem reputacji*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 356.
- Hillson D. (1997), *Toward a risk maturity model*, „The International Journal of Project & Business Risk Management”, Vol. 1, No. 1.
- International Standards for the Professional Practice of Internal Auditing* (2001), The Institute of Internal Auditors, Altamonte Springs.
- Juchniewicz M. (2009), *Dojrzałość projektowa organizacji*, Bizarre, Warszawa.
- Kania K. (2013), *Doskonalenie zarządzania procesami biznesowymi w organizacji z wykorzystaniem modeli dojrzałości i technologii informacyjno-komunikacyjnych*, Prace Naukowe Uniwersytetu Ekonomicznego, Katowice.
- 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, 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”, Vol. 59(1).
- Process Mining Manifesto* (2012) [w:] F. Daniel et al. (eds.) *Business Process Management Workshops*, „Lecture Notes in Business Information Processing”, Vol. 99.
- Racz N., Weippl E., Seufert A. (2010), *A Frame of Reference for Research of Integrated Governance, Risk, and Compliance (GRC)* [w:] B. Decker, I. Schamueller-Bichl (eds.), „Communications and Multimedia Security, Lecture Notes in Computer Science”, Vol. 6109.
- Röglinger M., Pöppelbuß J. (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), Association for Information Systems (AIS).

**IT ASPECTS OF THE PROCESS APPROACH AS A COMPONENT
MATURITY MODEL RISK MANAGEMENT**

Summary: The purpose of this article is – after the presentation of the essence of risk management and the role of audit in the risk management process – to demonstrate the maturity model for risk management and process aspects, and on this background characteristic of the support of this model by information technology used in the audit, including the innovative solutions developed by the author of the article.

Keywords: risk management, maturity model, process approach.