Standardy zarządzania ryzykiem w kontekście teorii Enterprise Risk Management (ERM)

Anna Reszke

Akademia Wymiaru Sprawiedliwości, Instytut Nauk o Zarządzaniu i Jakości

e-mail: anna.reszke@aws.edu.pl

Natalia Sobieska

Akademia Sztuki Wojennej, Szkoła Doktorska

e-mail: nsobieska@gmail.com

DOI: 10.65731/az-2026-0031

Streszczenie

Współczesne organizacje działają w środowisku charakteryzującym się dużą niepewnością i złożonością. Koncepcja Enterprise Risk Management (ERM) zakłada zintegrowane zarządzanie ryzykiem na wszystkich poziomach przedsiębiorstwa, wspierając podejmowanie spójnych decyzji. Artykuł podejmuje próbę porównania standardów zarządzania ryzykiem takich jak ISO i COSO ERM oraz zestawienie ich z koncepcją ustanowienia własnych standardów kontroli dla organizacji. Analiza została przeprowadzona z wykorzystaniem kryteriów obejmujących wartość praktyczną, koszty wdrożenia, możliwości certyfikacyjne, elastyczność oraz czas implementacji. Uzyskane wyniki wskazują, że najbardziej efektywnym rozwiązaniem mogą być wewnętrzne standardy organizacyjne, które zapewniają większą adaptacyjność oraz dopasowanie do indywidualnych potrzeb podmiotu. Jednocześnie podkreślono, iż współczesne zarządzanie ryzykiem nie powinno być postrzegane wyłącznie jako zbiór formalnych procedur, lecz jako zintegrowany sposób myślenia o funkcjonowaniu organizacji, ukierunkowany na antycypację zagrożeń, zdolność adaptacji do zmieniających się warunków oraz długofalowe utrzymanie stabilności.

Słowa kluczowe

ISO, COSO, FERMA, organizacja

Wstęp

Zarządzanie ryzykiem jest nieodzownym elementem efektywnego funkcjonowania współczesnych organizacji, zwłaszcza w warunkach rosnącej niepewności i złożoności otoczenia biznesowego. Rozwój standardów i ram zarządzania ryzykiem stanowi odpowiedź na potrzebę systematycznego podejścia do identyfikacji, oceny oraz kontroli zagrożeń wpływających na realizację celów przedsiębiorstw. Szczególne znaczenie w tym kontekście zyskała teoria Enterprise Risk Management (ERM), która promuje całościowe, zintegrowane zarządzanie ryzykiem na wszystkich szczeblach organizacyjnych, sprzyjając podejmowaniu świadomych i spójnych decyzji. Różnorodność dostępnych standardów, takich jak ISO 31000 czy COSO ERM, odzwierciedla zróżnicowane podejścia i wymagania sektorowe, co sprawia, że ich analiza i porównanie w świetle założeń ERM stanowi istotny obszar badań. Zrozumienie relacji między tymi ramami a koncepcją ERM umożliwia ocenę ich praktycznej wartości, identyfikację mocnych stron oraz ograniczeń, a także wspiera wybór najbardziej adekwatnych narzędzi do specyfiki danej organizacji.

Celem niniejszego artykułu jest próba porównania wybranych standardów zarządzania ryzykiem w kontekście teorii ERM, ze szczególnym uwzględnieniem ich struktury, zakresu oraz praktycznej użyteczności. W publikacji zostaną zostały zidentyfikowane kluczowe elementy determinujące skuteczność poszczególnych ram zarządzania ryzykiem oraz oceniono ich zgodność z holistycznym podejściem ERM, które integruje ryzyko na wszystkich szczeblach organizacji. Ponadto analiza pozwoliła na wskazanie różnic i podobieństw między standardami oraz ocenę ich potencjału adaptacyjnego do zróżnicowanych sektorów i warunków operacyjnych. W rezultacie artykuł dostarczy kompleksowej wiedzy, wspierającej świadome wybory dotyczące wdrażania efektywnych narzędzi zarządzania ryzykiem, sprzyjających zwiększeniu odporności i efektywności organizacji.

1. Teoretyczne podstawy zarządzania ryzykiem

Zarządzanie ryzykiem jest nieodłącznym elementem współczesnego zarządzania organizacjami i stanowi fundament ich skutecznego funkcjonowania niezależnie od branży, wielkości czy formy prawnej. W ujęciu klasycznym zarządzanie ryzykiem definiowane jest jako systematyczny proces identyfikowania, analizowania, oceny oraz kontrolowania zagrożeń, które mogą negatywnie wpłynąć na realizację wyznaczonych celów organizacyjnych [Jajuga, 2007, s. 23]. Proces ten ma na celu nie tylko minimalizację potencjalnych strat, ale także optymalizację szans

rozwojowych, co jest kluczowe dla długoterminowej stabilności i konkurencyjności przedsiębiorstwa. Norma ISO 31000:2018 definiuje zarządzanie ryzykiem jako koordynowane działania mające na celu kierowanie i kontrolę organizacji w odniesieniu do ryzyka [https://resilia.pl/blog/norma-iso-31000-zarzadzanie-ryzykiem-informacje-o-standardzie/, 01.07.2025r.]. Ta definicja podkreśla rolę zarządzania ryzykiem jako elementu systemu zarządzania organizacją, w którym ryzyko jest rozpatrywane w sposób integralny i świadomy. Podejście to wymaga zrozumienia ryzyka jako czynnika dynamicznego, który może mieć zarówno negatywne, jak i pozytywne konsekwencje dla organizacji, w zależności od sposobu zarządzania.

W tym kontekście warto wyjaśnić różnicę między standardem a normą. Standard to uznany zestaw zasad, wytycznych lub specyfikacji, opracowany zwykle przez organizacje branżowe, techniczne lub międzynarodowe, mający na celu ujednolicenie praktyk i zapewnienie spójności w określonym obszarze [Buczacki, 2016, s. 34-36]. Norma natomiast to dokument ustanowiony przez uznane instytucje normalizacyjne, takie jak ISO (Międzynarodowa Organizacja Normalizacyjna), który określa wymagania, wytyczne lub cechy, które muszą być spełnione przez produkty, procesy lub systemy [Buczacki, 2016, s. 36]. Normy mają często charakter bardziej formalny i mogą być podstawą do certyfikacji zgodności.

W literaturze przedmiotu coraz częściej akcentuje się, że zarządzanie ryzykiem nie powinno ograniczać się do działań reaktywnych, podejmowanych wyłącznie w odpowiedzi na wystąpienie zagrożeń. Wręcz przeciwnie, jest to proces proaktywny, który stanowi integralną część strategii organizacji, wspierając podejmowanie świadomych i przemyślanych decyzji na wszystkich poziomach zarządzania [Sopińska, 2010, s. 45]. Podejście to jest zgodne z koncepcją zarządzania strategicznego, gdzie ryzyko traktowane jest jako element decydujący o wyborze kierunków rozwoju, inwestycji czy alokacji zasobów. Skuteczne zarządzanie ryzykiem wpływa na wzrost efektywności operacyjnej poprzez eliminację lub ograniczenie wpływu niepożądanych zdarzeń, a także zwiększenie elastyczności organizacji w adaptacji do zmieniających się warunków rynkowych [Sopińska, 2010, s.52]. Ponadto, proces ten umożliwia ochronę kluczowych zasobów, w tym kapitału ludzkiego, finansowego oraz materialnego, co jest niezbędne do utrzymania ciągłości działania i realizacji misji organizacji. Z punktu widzenia zarządców i interesariuszy, zarządzanie ryzykiem wzmacnia również pozycję konkurencyjną organizacji, budując jej wiarygodność i zaufanie wśród partnerów biznesowych oraz klientów [Greczko, 2012, s. 88].

Współczesne wyzwania, takie jak globalizacja, rosnąca złożoność procesów biznesowych, postępująca digitalizacja oraz zmiany regulacyjne, powodują, że zarządzanie ryzykiem nabiera szczególnego znaczenia i staje się kluczowym na-

rzędziem zarządzania organizacją [Greczko, 2012, s.90]. Organizacje, które potrafią efektywnie identyfikować, analizować i zarządzać ryzykiem, zyskują przewagę konkurencyjną, są bardziej odporne na kryzysy i lepiej przygotowane na wykorzystanie nowych możliwości rynkowych [Greczko, 2012, s.92]. Tradycyjne zarządzanie ryzykiem opierało się głównie na działaniach o charakterze fragmentarycznym i funkcjonalnym, koncentrujących się na wybranych aspektach działalności organizacji, takich jak finanse, bezpieczeństwo operacyjne czy zgodność regulacyjna [Flieger, 2014, s.41]. Takie podejście często sprowadzało się do reakcji na zaistniałe incydenty i działań naprawczych, co w praktyce ograniczało zdolność organizacji do przewidywania i zarządzania ryzykami na poziomie strategicznym. Zarządzanie ryzykiem realizowane było w „silosach", gdzie poszczególne działy zajmowały się tylko ryzykami związanymi z ich własnymi kompetencjami, bez pełnej koordynacji i wymiany informacji między jednostkami [Flieger, 2014, s.45]. Skutkiem tego było ryzyko powielania działań, pomijania kluczowych zagrożeń oraz braku spójnego obrazu ryzyka na poziomie całej organizacji.

W odpowiedzi na rosnącą złożoność i zmienność otoczenia biznesowego, a także rosnące oczekiwania interesariuszy wobec zarządzania ryzykiem, rozwinięto koncepcję ERM, która wprowadza holistyczne i zintegrowane podejście do zarządzania ryzykiem [Woods, 2010, s.59]. ERM postuluje traktowanie ryzyka jako elementu przenikającego wszystkie obszary działalności organizacji, od operacji, przez finanse, po kwestie reputacyjne i strategiczne. Według standardu COSO ERM, jest to proces stosowany przez zarząd, kierownictwo oraz personel organizacji, mający na celu identyfikację potencjalnych zdarzeń mogących mieć wpływ na organizację, ocenę ryzyka w kontekście prawdopodobieństwa i skutków oraz koordynację odpowiedzi w celu minimalizacji strat i maksymalizacji szans [Krupski, 2013, s. 7-8]. Taka perspektywa pozwala na bardziej spójne zarządzanie ryzykiem, uwzględniające zarówno ryzyka negatywne, jak i pozytywne, które mogą wpłynąć na realizację celów organizacji. Kluczowym aspektem ewolucji zarządzania ryzykiem jest również podkreślenie roli kultury organizacyjnej oraz zaangażowania najwyższego szczebla zarządzania w procesy ERM [Mikes, 2014, s. 489]. Skuteczna implementacja ERM wymaga, aby zarząd i kierownictwo aktywnie wspierali i nadzorowali działania związane z zarządzaniem ryzykiem, a także budowali świadomość i odpowiedzialność za ryzyko na wszystkich poziomach organizacji. W literaturze wskazuje się, że kultura organizacyjna sprzyjająca otwartości na identyfikację i zgłaszanie ryzyk, a także promująca współpracę między działami, znacząco zwiększa efektywność zarządzania ryzykiem [Misztal, 2017, s. 45-60]. W efekcie organizacje stosujące ERM zyskują większą odporność na nieprzewidziane zdarzenia, elastyczność w reagowaniu na zmiany oraz lepsze dopasowanie

strategii do dynamicznego otoczenia biznesowego. Przykłady wdrożeń ERM w praktyce pokazują, że zintegrowane podejście do ryzyka przekłada się na poprawę procesów decyzyjnych, redukcję kosztów związanych z zarządzaniem kryzysowym oraz zwiększenie wartości dla akcjonariuszy [https://humansoft.pl/przyklady-wdrozen-systemow-erp/, 01.07.2025]. Współczesne organizacje, zwłaszcza działające na rynkach o wysokim poziomie regulacji i zmienności, coraz częściej traktują ERM jako narzędzie przewagi konkurencyjnej, które umożliwia nie tylko zabezpieczenie przed stratami, ale także aktywne wykorzystywanie pojawiających się szans rynkowych.

Teoria ERM opiera się na kilku fundamentalnych założeniach, które odróżniają ją wyraźnie od tradycyjnego podejścia do zarządzania ryzykiem. Pierwszym z nich jest wielowymiarowe postrzeganie ryzyka jako zjawiska zintegrowanego z celami organizacji na wszystkich szczeblach zarządzania – od strategicznego, przez taktyczny, aż po operacyjny [Różański, 2018, s.23-24]. Ryzyko nie jest już traktowane wyłącznie jako zagrożenie w wybranych obszarach funkcjonowania przedsiębiorstwa, lecz jako czynnik, który może wpływać na realizację wszystkich celów organizacji, co wymaga całościowego i spójnego podejścia. Drugim kluczowym założeniem jest systematyczność i ciągłość zarządzania ryzykiem. ERM zakłada, że proces ten powinien być nieustannie realizowany w ramach całej organizacji, z zastosowaniem sprawdzonych i ustandaryzowanych metod identyfikacji, oceny, monitorowania oraz kontrolowania ryzyka [Różański, 2018, s. 28]. Takie podejście pozwala na bieżąco reagować na zmiany w otoczeniu i wewnętrznych uwarunkowaniach, zapewniając w ten sposób wyższą odporność i elastyczność organizacji. Ponadto, teoria ERM kładzie wyraźny nacisk na podejście proaktywne. Wykorzystanie nowoczesnych narzędzi analitycznych, w tym modeli predykcyjnych, symulacji czy systemów wczesnego ostrzegania, umożliwia organizacjom przewidywanie potencjalnych zagrożeń oraz identyfikację pojawiających się szans [Jajuga, 2019, s. 112-113]. Dzięki temu proces zarządzania ryzykiem staje się nie tylko instrumentem zapobiegającym stratom, lecz również narzędziem wspierającym podejmowanie decyzji strategicznych i operacyjnych. Istotnym elementem teorii ERM jest również integracja zarządzania ryzykiem z procesem decyzyjnym na wszystkich poziomach organizacji, co wymaga przejrzystości, skutecznej komunikacji oraz rzetelnej dokumentacji podejmowanych działań [Jajuga, 2019, s.121]. Transparentność procesów ryzyka sprzyja budowaniu zaufania zarówno wewnątrz organizacji, jak i wśród zewnętrznych interesariuszy, a także ułatwia audyt oraz ciągłe doskonalenie systemów zarządzania ryzykiem. W literaturze przedmiotu coraz częściej podkreśla się, że ERM stanowi narzędzie tworzenia wartości dla interesariuszy organizacji poprzez zapewnienie stabilności, przewidywalności

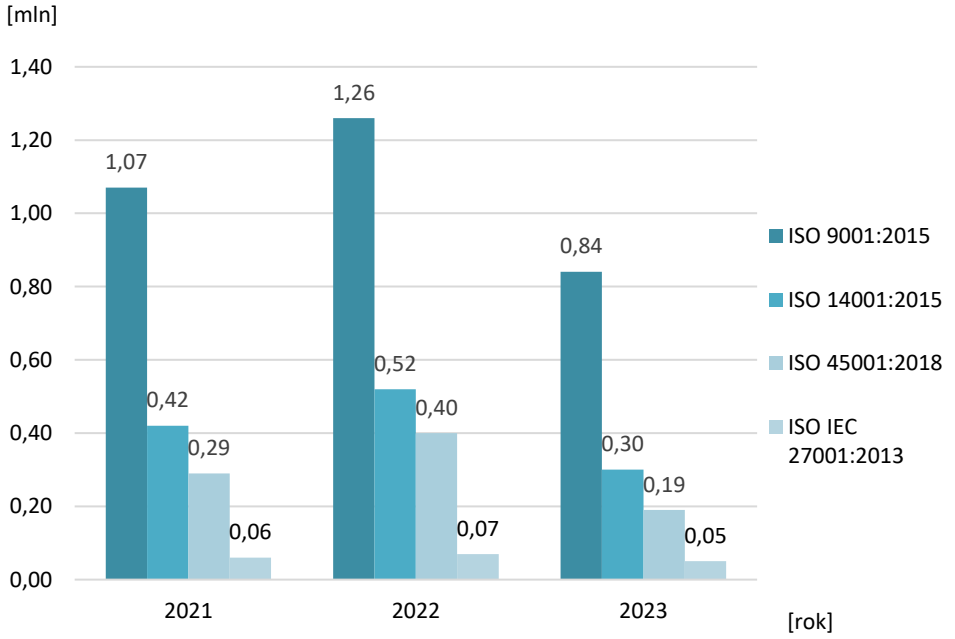
i bezpieczeństwa działalności [Misztal, 2017, s.75-76]. Tym samym teoria ta wykracza poza tradycyjne ramy zarządzania ryzykiem, oferując nowoczesne, kompleksowe podejście, które jest dostosowane do wyzwań współczesnego środowiska biznesowego, charakteryzującego się szybkim tempem zmian i rosnącą złożonością [Misztal, 2017, s. 78]. Podejście to umożliwia organizacjom nie tylko minimalizację negatywnych skutków ryzyka, lecz także aktywne wykorzystanie szans rynkowych, co stanowi kluczowy element długofalowego sukcesu.

2. Przegląd wybranych międzynarodowych standardów

Współczesne podejście do zarządzania ryzykiem, oparte na paradygmacie zintegrowanym, wymaga jasno zdefiniowanych ram, które umożliwiają skuteczne wdrażanie koncepcji ERM w różnych typach organizacji. Odpowiedzią na to zapotrzebowanie są międzynarodowe standardy, które nie tylko systematyzują procesy związane z identyfikacją i oceną ryzyka, lecz także wspierają instytucje w budowie kultury zarządzania ryzykiem, zorientowanej na wartość i długofalową odporność strategiczną. W literaturze oraz praktyce zarządczej szczególne znaczenie przypisuje się trzem dokumentom o charakterze referencyjnym: COSO ERM, ISO 31000:2018 oraz wytycznym opracowanym przez FERMA [Hopkin, 2018, s.45-47]. Choć różnią się konstrukcją i szczegółowością, wszystkie omawiane podejścia opierają się na założeniu, że ryzyko powinno być traktowane nie tylko jako zagrożenie, lecz także jako szansa. Zintegrowane, kompleksowe i spójne procesy zarządzania ryzykiem umożliwiają organizacjom skuteczne funkcjonowanie w środowisku charakteryzującym się nieprzewidywalnością i dynamicznymi zmianami.

Najbardziej rozpowszechnionymi standardami są te wydane przez ISO. Nazwa ta pochodzi od greckiego słowa „isos", oznaczającego „równy". Jest to organizacja pozarządowa, który od 1946 roku umożliwia handel i współpracę między ludźmi i firmami na całym świecie. Od początku istnienia dostarczyła 2588 standardów i innych produktów obejmujących niemal wszystkie aspekty technologii, zarządzania i produkcji [https://www.iso.org/about, 10.07.2025]. W praktycznym ujęciu, normy zawierające wytyczne ISO dotyczące różnych obszarów i systemów wdrażane są w organizacjach na całym świecie by optymalizować ich funkcjonowanie, ale równie po to, by uzyskać certyfikat potwierdzający dostosowanie procesów do wymogów. Ze względu na dużą wartość certyfikacji zero jedynkowo dzielącej przedsiębiorstwa na te z wdrożonymi standardami i niewdrożonymi, dochodzi do sytuacji, w której zdobycie dokumentu staje się ważniejsze niż wypracowanie realnie wpływających, korzystnych rozwiązań. Nie jest to również tani proces, co sprawia, że niektóre przedsiębiorstwa rezygnują z odnowienia certyfikatu. Liczba

certyfikatów wydanych przez jednostki certyfikujące zmieniała się w latach 2021-2023 (rys. 1).



Rys. 1. Liczba wydanych certyfikatów w latach 2021-2023

Źródło: https://ikmj.com/ile-certyfikatow-iso-wydano/, 10.07.2025.

Z powyższych danych wynika, że największą popularnością cieszy się ISO 9001 – System Zarządzania Jakością. Na podium znajdują się również ISO 14001 – System Zarządzania Środowiskowego oraz ISO 45001 – System Zarządzania Bezpieczeństwem i Higieną Pracy (BHP). ISO IEC 27001 dotyczy zaś Systemu Zarządzania Bezpieczeństwem Informacji (BI). Przeprowadzone badanie wskazuje na duży spadek liczby certyfikatów w roku 2023, ale nie jest to do końca prawda, ponieważ w danych nie uwzględniono informacji z chińskich jednostek certyfikujących, które stanowią znaczną ich część. Bardziej wartościowe porównanie będzie możliwe do przeprowadzenia, gdy zostanie stworzony raport za 2024 rok, uzupełniający te braki.

Wymienione, najpopularniejsze standardy ISO odnoszą się do jakości, środowiska, BHP i BI, podczas gdy norma odnosząca się do zarządzania ryzykiem,

31000 nie została ujęta. Powodem jest inna natura tych wytycznych, skierowanych nie tyle do organizacji jako podmiotu, ale do osób, które chcą rozumieć zasady zarządzania ryzykiem, poznać proces i umieć stosować tą wiedzę w praktyce. Spójne podejście do zarządzania ryzykiem na wszystkich poziomach pozwala identyfikować, oceniać i reagować na ryzyka w sposób uporządkowany. Rozpatrywanie tego pojęcia nie tylko jako zagrożeń, ale również możliwości zmienia sposób myślenia, dzięki czemu podejmowane decyzje są świadome, łatwiej realizuje się okazje do rozwoju i ogranicza wpływ błędów oraz odchyleń od planów. Zwiększa się również odporność organizacji poprzez konsekwentne dostosowanie do zmian zachodzących w dynamicznym otoczeniu.

Norma ISO 31000:2018 oferuje uniwersalne i przekrojowe ramy zarządzania ryzykiem, które mogą być wdrażane w dowolnym typie organizacji, niezależnie od jej wielkości, struktury wewnętrznej czy sektora działalności [https://www.pkn.pl/informacje/2018/04/zarzadzanie-ryzykiem, 26.03. 2026 r.]. Stanowi zbiór rekomendacji i najlepszych praktyk, które mogą być elastycznie adaptowane do konkretnych uwarunkowań instytucjonalnych. Elastyczność ta jest jednocześnie jedną z kluczowych zalet normy, pozwala bowiem na jej implementację zarówno w dużych korporacjach, jak i w małych i średnich przedsiębiorstwach, administracji publicznej, a nawet w sektorze non-profit. Dokument definiuje trzy główne elementy systemu zarządzania ryzykiem [https://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-polish-version.pdf, 08.07.2025, s.10]:

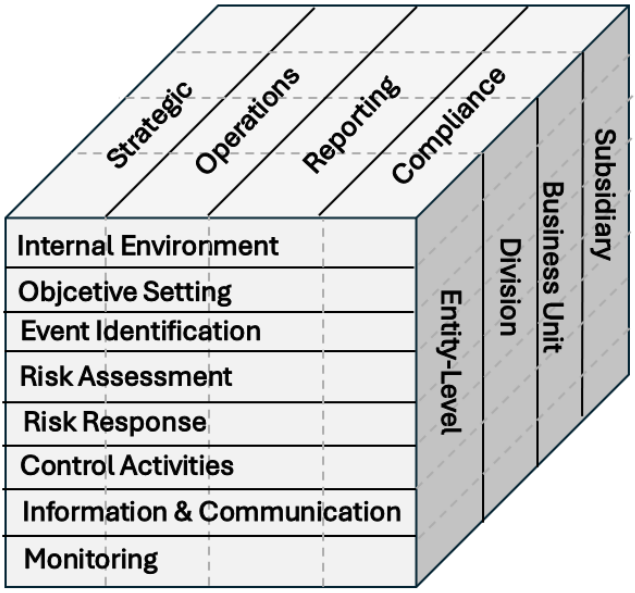
- zasady (principles), które określają fundamenty skutecznego zarządzania ryzykiem;
- ramy organizacyjne (framework), umożliwiające zintegrowanie procesu zarządzania ryzykiem z kulturą organizacyjną;
- procesy (process), opisujące sposób identyfikowania, analizowania, oceny i reagowania na ryzyko.

Norma ISO 31000:2018 kładzie szczególny nacisk na ciągłość, systematyczność oraz cykliczny charakter procesu zarządzania ryzykiem. W odróżnieniu od ram COSO ERM, ISO 31000 unika sztywnego określania ról i odpowiedzialności, akcentując zamiast tego elastyczność oraz możliwość adaptacji narzędzi zarządczych do specyficznego kontekstu organizacji. Ta cecha sprawia, że standard ten znajduje zastosowanie zarówno w sektorze prywatnym, jak i publicznym, co przyczynia się do jego statusu jednego z najczęściej cytowanych i wykorzystywanych standardów na poziomie globalnym. Dzięki swojej uniwersalności oraz elastyczności, norma ISO 31000:2018 stanowi solidną podstawę dla organizacji na całym świecie, umożliwiając im skuteczne wdrażanie zasad zarządzania ryzykiem, które

są precyzyjnie dostosowane do indywidualnych potrzeb oraz specyfiki prowadzonej działalności.

Stosowanie wytycznych ISO 31000 wspiera i uzupełnia systemy zarządzania: ISO 9001 wymaga identyfikacji ryzyk i szans dla systemu zarządzania jakością, ISO 14001 zawiera identyfikację ryzyk środowiskowych i szans na poprawę zgodności, ISO 45001 odnosi się do zarządzania ryzykiem zawodowym dla zdrowia i bezpieczeństwa, zaś ISO 27001 to podejście oparte na analizie ryzyka w kontekście bezpieczeństwa informacji. Niezbędnymi jest więc znajomość i stosowanie wytycznych ISO 31000 dotyczących zarządzania ryzykiem, by czerpać korzyści z wdrożenia każdej innej normy ISO.

Często przytaczanym w literaturze standardem dotyczącym zarządzania ryzykiem jest COSO II. Amerykańska organizacja Committee of Sponsoring Organizations of the Treadway Commission opracowała w 1992 r. raport (tzw. COSO I), który wyznaczył wieloletnie standardy w kontroli wewnętrznej, zdobywając popularność na całym świecie [Grzgorzewski, 2024, s.11]. Jego rozwinięciem było opublikowanie COSO II odnoszącego się do zarządzania ryzykiem w postaci modelu sześcianu z trzema płaszczyznami podzielonymi na elementy (rys. 2).



Rys. 2. Model COSO II (2004)

Źródło: opracowanie własne na podstawie [Lundqvisit, 2014, s. 5].

Publikacja ta zyskała szerokie uznanie wśród organizacji w ich działaniach na rzecz zarządzania ryzykiem. Jednak złożoność ryzyka uległa zmianie, pojawiły się nowe rodzaje ryzyka, a zarządy i kadra kierownicza zwiększyły swoją świadomość i nadzór nad zarządzaniem ryzykiem przedsiębiorstwa, jednocześnie domagając się udoskonalenia raportowania ryzyka [COSO, 2017]. Odpowiedzią na te zmiany było opublikowanie w 2017 roku nowego raportu. Zaktualizowana wersja zawiera 20 zasad osadzonych w pięciu obszarach (tab. 1).

Tab. 1. Zasady COSO 2017

Obszar	Zasady
Governance & Culture	1. Exercises Board Risk Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commitment to Core Values 5. Attracts, Develops, and Retains Capable Individuals
Strategy & Objective-Setting	6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives
Performance	10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14. Develops Portfolio View
Review & Revision	15. Assesses Substantial Change 16. Reviews Risk and Performance 17. Pursues Improvement in Enterprise Risk Management
Inofrmation, Comunication & Reporting	18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance

Źródło: opracowanie własne na podstawie [COSO, 2017, s. iii].

Standard ten podkreśla rolę zarządu i najwyższego kierownictwa w tworzeniu kultury świadomego ryzyka, a także konieczność integrowania ryzyka z procesem planowania strategicznego [Misztal, 2017, s.120-121]. COSO ERM zakłada, że ryzyko powinno być rozpatrywane zarówno w kontekście zagrożeń, jak i możliwości, co odróżnia ten model od tradycyjnych, defensywnych podejść do zarządzania ryzykiem [Misztal, 2017, s. 123]. Kluczowym elementem jest także dynamiczne dostosowywanie systemu zarządzania ryzykiem do zmieniających się uwarunkowań wewnętrznych i zewnętrznych [Różański, 2018, s. 55-58].

Publikacje wydawane po 2017 roku w dużej mierze wciąż odwołują się do modelu z 2004 roku, aktualizacja nie jest tak szeroko omawiana i praktykowana. Posiada jednak niewątpliwie ważne zmiany. Na wyróżnienie zasługuje zwiększenie nacisku na komunikację – z czterech funkcji zarządzania, jakimi są planowanie, organizowanie, motywowanie i kontrola, ta trzecia wymaga współcześnie dużej uwagi. Wytyczne stosunkowo łatwo jest wprowadzić do procesu, przygotować plan, przydzielić zasoby, zastosować wskaźniki do kontroli. Motywowanie jest najmniej wymierne, łatwo powiedzieć: „bądź przywódcą", stworzyć system motywacyjny obejmujące finansowe motywacje, trudniej zaś sprawić, by osoba odpowiedzialna za dane zadanie była w nie faktycznie zaangażowana przy zachowaniu realnej efektywności. Szczególnie jeśli chodzi o zarządzanie ryzykiem, a więc sytuacje, które jedynie mogą się wydarzyć. W praktyce gospodarczej często nie ma na to czasu, tu i teraz dzieje się wystarczająco dużo by zająć całą energię.

Podobnie jak ISO 3100, COSO II to rodzaj standardu, który można poznać na szkoleniach i uzyskać certyfikat na osobę, potwierdzający znajomość wytycznych, nie certyfikuje się organizacji.

W kontekście europejskim, gdzie obowiązują specyficzne regulacje oraz zróżnicowane uwarunkowania kulturowe i gospodarcze, standard ISO 31000 jest systematycznie uzupełniany przez wytyczne opracowane przez Federation of European Risk Management Associations (FERMA) [Różański, 2018, s. 11]. FERMA, funkcjonująca jako platforma koordynacji i współpracy między krajowymi stowarzyszeniami menedżerów ryzyka, skupia się na promowaniu rozwiązań zarządczych uwzględniających specyfikę europejskiego kontekstu [Okuniewski, 2007, s. 3]. Wytyczne FERMA kładą szczególny nacisk na rolę menedżerów ryzyka jako kluczowych aktorów procesów decyzyjnych, podkreślając jednocześnie znaczenie efektywnej komunikacji, współpracy między funkcyjnej oraz konieczność adaptacji narzędzi ERM do lokalnych regulacji prawnych oraz specyfiki rynków. W ten sposób standardy FERMA pełnią funkcję komplementarnego uzupełnienia wobec normy ISO 31000, dostarczając praktycznych wskazówek i ram postępowania umożliwiających efektywne wdrażanie zintegrowanego zarządzania ryzykiem na poziomie europejskim [Okuniewski 2007, s. 4]. Dzięki temu menedżerowie ryzyka otrzymują narzędzia pozwalające na harmonizację ogólnych standardów z wymaganiami oraz realiami poszczególnych krajów, co sprzyja skuteczniejszemu zarządzaniu ryzykiem w wieloaspektowym środowisku europejskim.

Kolejnymi popularnymi standardami zarządzania ryzykiem są National Institute of Standards and Technology Risk Managment Framework (NIST RMF) skupiający się na cyberbezpieczeństwie, Basel III (opracowany przez Bazylejski Komitet Nadzoru Bankowego) dotyczący bankowości, czy Solvency II (Directive

2009/138/EC w sprawie podejmowania i prowadzenia działalności w zakresie ubezpieczeń i reasekuracji) ukierunkowany na ubezpieczenia. Poza wymienionymi, istnieją również branżowe wytyczne dotyczące energetyki, inżynierii, IT, zdrowia, czy żywności – szacunkowo istnieje 60 – 80 oficjalnych norm zarządzania ryzykiem. Jeśli tego byłoby mało, duże korporacje wprowadzają własne, wewnętrzne standardy, uwzględniające specyfikę organizacji, dostosowując wytyczne do praktyki gospodarczej realizowanych zadań. Takie podejście zdecydowanie zwiększa korzyści wynikające z wdrożenie dopasowanych standardów, pozwala też na zachowanie elastyczności i szybką reakcję na zmianę w otoczeniu – nie tyle procesu, co całego standardu, co jest niezależne od organizacji w przypadku stosowania uniwersalnych standardów. Niemniej wartość takich wytycznych zależna jest od wysiłku, wiedzy i doświadczenia tych, którzy je tworzą.

3. Analiza porównawcza wybranych standardów zarządzania ryzykiem

Standardy tworzone są przez organizacje, można je więc skategoryzować jako produkt, dostarczany przez różne podmioty gospodarcze. Na potrzeby badania opracowano autorską, subiektywną metodę oceny standardów dedykowanych organizacjom, opartą na pięciu kryteriach: wartości praktycznej wdrożenia, kosztach wdrożenia i utrzymania, możliwości uzyskania certyfikacji o znaczeniu marketingowym, elastyczności względem zmian otoczenia oraz czasie implementacji (tab. 2).

Porównanie przeprowadzono z wykorzystaniem skali punktowej, w której najwyższą ocenę (3 punkty) przypisywano rozwiązaniu dominującemu w danej kategorii, natomiast najniższą (1 punkt) rozwiązaniu najsłabszemu. Dodatkowo, w celu zwiększenia waloru analitycznego, poszczególnym kryteriom nadano zróżnicowane wagi.

Tab. 2. Porównanie standardów

Kategoria	Waga	ISO		COSO		Wewnętrzny standard	
Wartość praktyczna	40%	1	0,4	2	0,8	3	1,2
Koszt	30%	3	1,05	1	0,35	2	0,7
Certyfikacja	15%	3	0,45	2	0,3	1	0,15
Elastyczność	10%	1	0,05	2	0,1	3	0,15
Czas	5%	3	0,15	2	0,1	1	0,05
Razem	**100%**	**11**	**2,1**	**9**	**1,65**	**10**	**2,25**

Źródło: opracowanie własne.

Wartość praktyczna, rozumiana jako rzeczywiste korzyści wynikające z prawidłowego wdrożenia i stosowania standardów zarządzania ryzykiem, może być analizowana w wielu wymiarach. Do najistotniejszych należą aspekty finansowe, w tym oszczędności osiągane dzięki optymalizacji procesów oraz skróceniu czasu realizacji działań, możliwe do wyrażenia chociażby w kategoriach roboczogodzin. Równie istotna jest ocena jakościowa, obejmująca m.in. poziom satysfakcji pracowników oraz klientów.

Jednocześnie należy podkreślić, że nie istnieje jednoznaczna odpowiedź na pytanie, który z analizowanych standardów charakteryzuje się najwyższą wartością praktyczną. Przeprowadzenie obiektywnych badań porównawczych w tym zakresie jest utrudnione, przede wszystkim ze względu na ograniczoną porównywalność wyników osiąganych przez różne organizacje funkcjonujące w odmiennych warunkach.

Można jednak przyjąć, że rozwiązania dostosowane do specyficznych potrzeb i możliwości danej organizacji wykazują większy potencjał praktyczny niż implementacja ogólnych, uniwersalnych wytycznych. W tym kontekście standardy o charakterze wewnętrznym mogą oferować wyższą użyteczność operacyjną. Należy również zauważyć, iż koncepcja COSO jest w większym stopniu ukierunkowana na potrzeby dużych organizacji, w szczególności korporacji, podczas gdy standardy ISO zachowują bardziej uniwersalny charakter i mogą być stosowane w szerokim spektrum podmiotów.

Kategoria kosztu stanowi istotny element analizy porównawczej i może być rozpatrywana zarówno na poziomie ogólnym, jak i w odniesieniu do konkretnych przypadków, poprzez pozyskanie ofert rynkowych oraz opracowanie budżetu dla projektu wdrożeniowego, w tym także dla wariantu obejmującego opracowanie wewnętrznych standardów organizacyjnych.

W ujęciu ogólnym można przyjąć, że wdrożenie koncepcji COSO wiąże się z wyższymi kosztami niż implementacja standardów ISO. Natomiast w przypadku projektowania własnych wytycznych poziom nakładów finansowych ma charakter wysoce zindywidualizowany i pozostaje w ścisłej zależności z czasem przeznaczonym na realizację przedsięwzięcia. Wydłużenie horyzontu czasowego umożliwia bowiem optymalizację zaangażowania zasobów kadrowych, poprzez ograniczenie liczby pracowników lub zmniejszenie wymiaru ich zaangażowania.

W analizie przyjętej w tabeli 2 założono, iż opracowanie wewnętrznych standardów będzie rozwiązaniem relatywnie mniej kosztownym, przy jednoczesnym wydłużeniu czasu realizacji. Jednocześnie, ze względu na wysoką popularność standardów ISO oraz szeroką dostępność wyspecjalizowanych podmiotów dorad-

czych i jednostek certyfikujących, czas ich wdrożenia można uznać za relatywnie krótszy w porównaniu z implementacją koncepcji COSO.

Ocena w zakresie certyfikacji ma charakter relatywnie jednoznaczny. Standardy z rodziny ISO umożliwiają uzyskanie formalnego certyfikatu, który stanowi istotny element budowania wiarygodności organizacji oraz może pełnić funkcję narzędzia o charakterze marketingowym. W przypadku koncepcji COSO, pomimo braku formalnego mechanizmu certyfikacji, samo odwołanie się do jej wdrożenia w komunikacji biznesowej jest powszechnie rozpoznawalne i interpretowane jako stosowanie uznanych, międzynarodowych wytycznych w zakresie zarządzania ryzykiem. Natomiast wewnętrzne standardy organizacyjne, ze względu na ich zindywidualizowany oraz często niejednoznaczny charakter, nie posiadają analogicznej wartości komunikacyjnej. Ich rozpoznawalność w otoczeniu zewnętrznym jest ograniczona, co sprawia, iż nie są one postrzegane jako istotny wyróżnik ani dodatkowa wartość w kontekście relacji biznesowych.

Ocena elastyczności, rozumianej jako zdolność dostosowywania działań do obowiązujących wytycznych oraz modyfikowania samych wytycznych w odpowiedzi na zmieniające się uwarunkowania, nie budzi istotnych wątpliwości interpretacyjnych. W tym kontekście szczególną przewagę wykazują wewnętrzne standardy organizacyjne, które mogą być na bieżąco adaptowane zarówno do zmian zachodzących wewnątrz organizacji, jak i w jej otoczeniu zewnętrznym.

Odmiennie przedstawia się sytuacja w przypadku standardów opracowywanych przez organizacje takie jak ISO czy COSO, których aktualizacja jest procesem czasochłonnym i sformalizowanym. W odniesieniu do standardów ISO dodatkowym czynnikiem ograniczającym elastyczność jest konieczność ścisłego stosowania aktualnych wersji dokumentów w celu utrzymania certyfikacji. Z kolei koncepcja COSO, mimo braku formalnych mechanizmów certyfikacyjnych, pozostawia większą swobodę interpretacyjną i adaptacyjną, gdyż organizacje nie podlegają bezpośredniej weryfikacji zgodności przez zewnętrzne jednostki certyfikujące.

Zaproponowana koncepcja oceny, pomimo swojego wstępnego i częściowo subiektywnego charakteru, może stanowić punkt wyjścia do dalszych, pogłębionych badań w zakresie porównywania efektywności standardów zarządzania ryzykiem, w szczególności z uwzględnieniem specyfiki różnych typów organizacji oraz uwarunkowań ich funkcjonowania.

Podsumowanie

Dobór odpowiednich ram zarządzania ryzykiem powinien uwzględniać specyfikę organizacji, w tym jej cele strategiczne, strukturę organizacyjną, kulturę we-

wnętrzną oraz uwarunkowania regulacyjne i rynkowe, w jakich dana jednostka funkcjonuje. W praktyce oznacza to konieczność świadomego wyboru między standardami o wysokim stopniu sformalizowania, jak ISO 31000, a bardziej elastycznymi modelami wewnętrznymi, które pozwalają na precyzyjne dostosowanie procedur do realiów konkretnej organizacji. Co istotne, skuteczne zarządzanie ryzykiem nie polega jedynie na wyborze konkretnego standardu, lecz na jego właściwej implementacji, integracji z procesami decyzyjnymi oraz konsekwentnym doskonaleniu w czasie. W tym kontekście organizacje coraz częściej sięgają po podejścia hybrydowe, łącząc elementy różnych modeli, np. strukturę i systematyzację ISO z elastycznością rozwiązań wewnętrznych oraz akcentami strategicznymi charakterystycznymi dla COSO ERM. Z perspektywy długoterminowej odporności organizacyjnej, wdrożenie skutecznego systemu zarządzania ryzykiem nie tylko wspiera osiąganie celów operacyjnych i strategicznych, lecz także sprzyja budowaniu zaufania interesariuszy, poprawia jakość zarządzania oraz zwiększa adaptacyjność organizacji w obliczu niepewności i dynamicznych zmian otoczenia.

Wybór i wdrożenie określonego standardu zarządzania ryzykiem wiąże się również z konsekwencjami organizacyjnymi, finansowymi i kulturowymi. W przypadku standardów międzynarodowych, takich jak ISO 31000, istotnym atutem jest ich uniwersalność, transparentność oraz możliwość uzyskania certyfikacji, co bywa szczególnie istotne w relacjach z partnerami zewnętrznymi i w przetargach publicznych. Z kolei podejścia autorskie, rozwijane wewnątrz organizacji, oferują większą elastyczność, ale wymagają silnego zaplecza eksperckiego, dojrzałej kultury organizacyjnej i konsekwentnego monitorowania skuteczności wdrożonych rozwiązań.

Niezależnie od wybranej ścieżki, kluczowym warunkiem powodzenia systemu zarządzania ryzykiem pozostaje jego realne zakorzenienie w strukturach decyzyjnych i operacyjnych organizacji. Formalne przyjęcie standardu nie gwarantuje jeszcze wzrostu efektywności, jeśli nie towarzyszy mu zmiana świadomości kadry kierowniczej, odpowiednie szkolenia pracowników oraz sprawny system komunikacji ryzyka. Dlatego też nowoczesne zarządzanie ryzykiem powinno być postrzegane nie jako zestaw procedur, lecz jako sposób myślenia o organizacji — zorientowany na przewidywanie, adaptację i długofalową stabilność.

ORCID iD

Anna Reszke: https://orcid.org/0000-0003-3035-6748

Natalia Sobieska: https://orcid.org/0009-0004-4486-7447

Literatura

1. Buczacki A. (2016), *Zarządzanie jakością i normy ISO*, PWE, Warszawa.
2. Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2017), *Enterprise Risk Management – Integrated Framework.*
3. Federation of European Risk Management Associations (FERMA) (2003), *Standard zarządzania ryzykiem*, tłumaczenie: FERMA, https://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-polish-version.pdf [08.07.2025].
4. Flieger M. (2014), *Zarządzanie ryzykiem operacyjnym w przedsiębiorstwie*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań.
5. Greczko T. (2012), *Zarządzanie ryzykiem jako element strategii organizacji*, Difin, Warszawa.
6. Grzegorzewski J. (2024), *Kontrola wewnętrzna oparta na ramach COSO jako przedmiot badania audytu wewnętrznego,* w: Przybylska J. M., Kańduła S., Bogucka I., (red.), *Audyt wewnętrzny narzędziem ułatwiającym zarządzanie organizacją*, WUE, Poznań.
7. Hopkin A. (2018), *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*, 5th edition, Kogan Page, London.
8. https://humansoft.pl/przyklady-wdrozen-systemow-erp/ [01.07.2025].
9. https://ikmj.com/ile-certyfikatow-iso-wydano/ [10.07.2025].
10. https://www.iso.org/about [10.07.2025].
11. Jajuga K. (2007), *Zarządzanie ryzykiem*, Wydawnictwo Naukowe PWN, Warszawa.
12. Jajuga K. (2019), *Zarządzanie ryzykiem finansowym przedsiębiorstwa*, Wydawnictwo Naukowe PWN, Warszawa.
13. Krupski R. (red.), (2013), *Zarządzanie strategiczne. Quo vadis?*, Prace Naukowe Wałbrzyskiej Wyższej Szkoły Zarządzania i Przedsiębiorczości, Wałbrzych.
14. Lundqvisit S. A. (2014), *Abonding Silos for integration: Impementing Enterprise Risk Management and Risk* Governance, Lund University.
15. Mikes M. (2014), *The Culture of Risk Management: How Leadership Shapes Risk Awareness*, Journal of Risk Research, nr 17(4), s. 489–511.
16. Misztal A. (2017), *Kultura organizacyjna a zarządzanie ryzykiem przedsiębiorstwa*, w: Misztal A. (red.), *Zarządzanie ryzykiem w przedsiębiorstwie*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków, s. 45-60.
17. Misztal A. (2017), *Zarządzanie ryzykiem przedsiębiorstwa jako element tworzenia wartości dla interesariuszy*, w: Misztal A. (red.), *Zarządzanie ryzykiem w przedsiębiorstwie*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków, s. 75-76.

18. Okuniewski M. (2007), *Standardy zarządzania ryzykiem*, Uniwersytet Ekonomiczny w Katowicach, Katowice.
19. Różański M. (2018), *Enterprise Risk Management – założenia i wyzwania*, w: Jajuga K. (red.), *Zarządzanie ryzykiem w organizacji*, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice, s. 23-24.
20. Różański M. (2018), *Zarządzanie ryzykiem w organizacji – podejście adaptacyjne*, w: Jajuga K. (red.), *Zarządzanie ryzykiem w organizacji*, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice, s. 23-24.
21. Sopińska A., Wachowska M. (2010), *Zarządzanie ryzykiem w przedsiębiorstwie*, Oficyna Wolters Kluwer business, Warszawa.
22. Woods J. A. (2010), *Zarządzanie ryzykiem w praktyce. Kompleksowe podejście do identyfikacji, oceny i kontroli ryzyka*, Wolters Kluwer, Warszawa.

Risk Management Standards in the Context of Enterprise Risk Management (ERM) Theory

Abstract

Contemporary organizations operate in an environment characterized by high uncertainty and complexity. The concept of Enterprise Risk Management (ERM) assumes an integrated approach to risk management across all levels of an enterprise, supporting coherent decision-making processes. This article attempts to compare risk management standards such as ISO and COSO ERM and to juxtapose them with the concept of establishing internal control standards within an organization. The analysis was conducted using criteria including practical value, implementation costs, certification opportunities, flexibility, and implementation time. The results indicate that internally developed organizational standards may constitute the most effective solution, as they provide greater adaptability and alignment with the specific needs of a given entity. At the same time, it is emphasized that contemporary risk management should not be perceived solely as a set of formal procedures, but rather as an integrated way of thinking about organizational functioning, focused on anticipating threats, adapting to changing conditions, and maintaining long-term stability.

Key words

ISO, COSO, FERMA, organizacja, organization