Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie
Research Reviews of Czestochowa University of Technology. Management

Nr 50 (2023), s. 98-112, ISSN: 2083-1560
DOI: 10.17512/znpcz.2023.2.08, https://znz.pcz.pl/

Nadesłanie artykułu: 10.05.2023; Poprawa artykułu: 05.06.2023;
Akceptacja: 07.06.2023; Publikacja: 30.06.2023.

SIEĆ MIĘDZYORGANIZACYJNA WOBEC CZYNNIKÓW RYZYKA: STUDIUM PRZYPADKU PLATFORMY ARIBA NETWORK

Kacper Sieciński[1*]

[1] Uniwersytet Warmińsko-Mazurski w Olsztynie, Wydział Nauk Ekonomicznych, Polska

Streszczenie: Sieci międzyorganizacyjne w modelu business to business (B2B) charakteryzują się dużą liczbą uczestników, co wiąże się z szeregiem czynników ryzyka, które mogą wpłynąć na procesy biznesowe w tych sieciach. Z tego względu ważne jest, aby dokładnie zbadać te determinanty i opracować odpowiednie strategie minimalizacji zagrożeń. Celem badania jest zidentyfikowanie czynników ryzyka w sieci międzyorganizacyjnej funkcjonującej w ramach platformy Ariba Network oraz ocena wpływu tych elementów na procesy biznesowe w tej sieci. W ramach badania przeanalizowano mechanizmy minimalizacji zagrożeń stosowane w badanym podmiocie oraz narzędzia służące do zwiększenia bezpieczeństwa procesów zachodzących w sieci. Praktyka przeciwdziałania zagrożeniom wewnętrznym oraz zewnętrznym w badanej platformie opiera się na wyróżnieniu czterech głównych kategorii potencjalnych niebezpieczeństw. Umiejętność identyfikacji oraz prognozy prawdopodobieństwa wystąpienia ryzyka może okazać się kluczowa do utrzymania stabilności procesów biznesowych. Organizacje korzystające z zasobów platformy Ariba Network są monitorowane, a pozyskane informacje są przetwarzane w celu opracowania przyszłych strategii zapobiegania zagrożeniom. Wiedza pozyskana w konsekwencji przeprowadzonego badania może okazać się przydatna dla przedsiębiorstw, które działają w modelu biznesowym B2B, a chcą minimalizować ryzyko wynikające z wystąpienia nieprawidłowości we współpracy pomiędzy członkami sieci międzyorganizacyjnej.

Słowa kluczowe: business to business (B2B), czynniki ryzyka, e-commerce, sieci międzyorganizacyjne

Kod klasyfikacji JEL: D81, D85, D89

[1] Kacper Sieciński, mgr, ul. Dworcowa 61/21, 10-437 Olsztyn, Polska, kacper.siecinski@uwm.edu.pl
https://orcid.org/0000-0001-8484-0741
* Autor korespondencyjny: Kacper Sieciński, kacper.siecinski@uwm.edu.pl

DOI: 10.17512/znpcz.2023.2.08

Wprowadzenie

Sieci międzyorganizacyjne, będące jednym z kierunków ewolucji współczesnych stosunków gospodarczych, stanowią kompleksowe związki biznesowe pomiędzy różnymi organizacjami, które mogą przyczynić się do wzrostu efektywności, konkurencyjności oraz innowacyjności przedsiębiorstw. Jednym z przykładów takiej sieci jest platforma Ariba Network (https://www.sap.com/…), będąca globalnym rynkiem zakupowym i sprzedażowym, która umożliwia firmom nawiązywanie współpracy handlowej na zasadach elektronicznego biznesu. Organizacja System Analysis Program Development (SAP) wspomaga organizacje w zarządzaniu procesami zaopatrzenia, współpracy w budowie łańcuchów dostaw, zarządzaniu dostawcami, polityki prywatności, globalnej ekspansji oraz zarządzaniu umowami i katalogami.

Pomimo korzyści wynikających z uczestnictwa w sieciach międzyorganizacyjnych istnieją także potencjalne czynniki ryzyka, które mogą wpłynąć na ich działanie i wyniki. W kontekście platformy Ariba Network obecne są pewne elementy funkcjonowania sieci, które mogą wiązać się z ryzykiem, takie jak: zależność od technologii informatycznych, ochrona danych osobowych, zgodność z regulacjami prawno-podatkowymi, zarządzanie technologią i produktami, różnorodność kulturowa i geograficzna, a także bezpieczeństwo cybernetyczne.

W związku z powyższym celem badania jest zidentyfikowanie czynników ryzyka w sieci międzyorganizacyjnej oraz ocena wpływu tych czynników na procesy biznesowe w tej sieci. W pracy wykorzystano zarówno teoretyczne podejście oparte na literaturze naukowej, jak i praktyczne doświadczenia związane z zarządzaniem sieciami międzyorganizacyjnymi oraz funkcjonowaniem platformy Ariba Network. Analiza ta ma na celu zidentyfikowanie, ocenę oraz zrozumienie istoty i skutków tych czynników ryzyka oraz wniesienie wkładu w rozwijający się obszar badań związanych z zarządzaniem sieciami międzyorganizacyjnymi i platformami e-biznesowymi.

Przegląd literatury

Sieci międzyorganizacyjne to suma formalnych i nieformalnych relacji między organizacjami, jako niezależnymi podmiotami w układzie powiązań pomiędzy jej członkami. Jest to współdziałanie trzech lub więcej jednostek, które nie muszą mieć określonego wspólnego celu, ale są zaangażowane w złożone interakcje oraz wymianę zasobów materialnych i niematerialnych. Sieci międzyorganizacyjne są efektem rozwijającego się rynku, który determinuje nawiązywanie współpracy pomiędzy organizacjami w celu podniesienia swojej konkurencyjności (Raab, 2018). Podstawową wartością w sieciach międzyorganizacyjnych jest podejście relacyjne w tworzeniu przewagi na rynku, zgodnie z którym strategiczna współpraca pomiędzy jednostkami w sieci jest głównym sposobem poprawy wyników uczestników. Kooperacja organizacji uczestniczących w sieci umożliwia uzyskanie dostępu do zaawansowanych technologii, podział kosztów rozwoju nowych kompetencji oraz mobilizację wspólnych komplementarnych sił (Światowiec-Szczepańska, 2016).

Za główne wyróżniki sieci międzyorganizacyjnej można przyjąć:
- dążenie do współdziałania, przy jednoczesnej stosunkowo dużej, a nawet pełnej autonomii decyzyjnej podmiotów i przy sporym zakresie konkurencji;
- wykorzystanie mechanizmów rynkowej koordynacji działań;
- zwiększenie potencjału innowacyjności w obszarach organizacyjno-zarządczych;
- minimalizowanie kosztów transakcyjnych;
- wspólnotę celów oraz wynikający z niej wysoki poziom zaufania i wzajemności;
- brak dominującej roli powiązań kapitałowych;
- niski poziom integracji pionowej i hierarchii między uczestnikami dysponującymi możliwie zróżnicowanym zestawem zasobów i kompetencji;
- ograniczenie lub wyeliminowanie kosztów hierarchii;
- naturalną rynkową elastyczność całej sieci i jej węzłów (Niemczyk et al., 2012).

Sieci międzyorganizacyjne muszą dostosowywać się do zmieniającego się środowiska, w którym funkcjonują, dlatego w literaturze naukowej zwraca się szczególną uwagę na to, aby relacje pomiędzy uczestnikami sieci charakteryzowały się dynamicznością. Pojęcia tego używa się nie tylko w kontekście modelowania relacji, ale również w odniesieniu do ich ewolucji (Bergenholtz & Waldstrøm, 2011). Dynamiczność rozpatrywana jest również ze względu na czas współpracy danej grupy podmiotów i oznacza ukierunkowanie poszczególnych przedsiębiorstw na określony fragment wartości dodanej sieci międzyorganizacyjnej oraz jednoczesne poszukiwanie innych wyspecjalizowanych organizacji, które są w stanie uzupełnić brakujące luki strukturalne w sieci (Adamik, 2021). W szerszym ujęciu istotę sieci międzyorganizacyjnych oraz relacji pomiędzy organizacjami omawiają w monografiach tacy autorzy, jak: Barczak (2020) Oliński (2019), Krechowicz i Kiliańska (2019) oraz Hejduk (2014).

W związku z dynamicznością sieci międzyorganizacyjnych należy cyklicznie analizować wpływ czynników wewnętrznych oraz zewnętrznych na funkcjonowanie relacji w sieci. Efektywne zarządzanie ryzykiem w sieciach międzyorganizacyjnych jest kluczowe dla zapewnienia ich długoterminowej stabilności. Dlatego też członkowie sieci powinni dokładnie przeanalizować czynniki ryzyka i wdrożyć właściwe strategie i metody zarządzania, aby zminimalizować wpływ ryzyka na funkcjonowanie sieci. Skuteczne zarządzanie ryzykiem w sieciach międzyorganizacyjnych wymaga koordynacji działań pomiędzy różnymi podmiotami oraz stosowania elastycznych strategii biznesowych, które pozwalają na szybką adaptację do zmieniających się okoliczności (Wasiluk & Tomaszuk, 2020). Każde zagrożenie jest potencjalnym źródłem ryzyka, które badacze próbują klasyfikować w odrębne grupy, aby ułatwić pracę z nimi. Ogólnie skuteczność organizacji procesu zarządzania ryzykiem zależy w dużej mierze od jego klasyfikacji, dostarczając przesłanek do efektywnego zastosowania odpowiednich metod i technik zarządzania nim (Iwaszczuk, 2021).

W literaturze naukowej występuje kilka klasyfikacji ryzyka. Borkowski (2008) zaproponował najprostszy podział ze względu na szczegółowość analizy podmiotu:
- ryzyko ogólne (polityczne, polityki wewnętrznej, polityki makroekonomicznej, warunków naturalnych);
- ryzyko specyficzne dla danej gałęzi (rynków surowców i zbytu, konkurencji);
- ryzyko charakterystyczne dla danego przedsiębiorstwa (operacyjne, badań i rozwoju, kredytowe, behawioralne, realizacji projektów).

DOI: 10.17512/znpcz.2023.2.08

W Tabeli 1 przedstawiono szczegółową klasyfikację ryzyka według Kotłowskiej (2016). Autorka postuluje, że mając na względzie ocenę kondycji przedsiębiorstwa z perspektywy możliwych do osiągnięcia wyników finansowych na poszczególnych szczeblach rachunku przepływów pieniężnych, bardziej wszechstronnym podejściem jest klasyfikacja ryzyka na trzy kategorie: ryzyko operacyjne, strategiczne oraz finansowe. Taka segmentacja umożliwia bezpośrednią analizę wpływu ryzyka na wartość przedsiębiorstwa.

Tabela 1. Klasyfikacja szczegółowa według kategorii ryzyka operacyjnego, strategicznego i finansowego

Kategorie ryzyka	Główne	Operacyjne	Strategiczne	Finansowe
	Szczegółowe	– ryzyko zarządzania i działalności operacyjnej – ryzyko operacyjne aktywów – ryzyko ludzkie – ryzyko związane z umowami – ryzyko bezpieczeństwa informacji – ryzyko w obszarze czynników naturalnych	– ryzyko polityczne – ryzyko inwestycyjne – ryzyko zrównoważonego rozwoju – ryzyko zabezpieczenia i refinansowania	– ryzyko walutowe – ryzyko cenowe – ryzyko wolumenu sprzedaży – ryzyko ceny i wolumenu paliw – ryzyko inflacji – ryzyko rynkowe – ryzyko kredytowe – ryzyko płynności – ryzyko stopy procentowej

Źródło: Opracowanie własne na podstawie (Kotłowska, 2016)

Ryzyko operacyjne można zdefiniować jako ryzyko wynikające z niedoskonałości wewnętrznych procesów, niskiego poziomu wiedzy i umiejętności pracowników oraz awarii systemów informatycznych, a także z czynników zewnętrznych. Ryzyko strategiczne dotyczy elementów mających szczególne znaczenie w procesie kreowania wartości przedsiębiorstwa. Na tę kategorię ryzyka wpływ mają m.in. regulacje prawne, sposób wykonywania inwestycji, zabezpieczenia oraz polityka zrównoważonego rozwoju. Ryzyko finansowe związane jest ze zmianami w strukturze źródeł finansowania działalności przedsiębiorstwa, czyli ze zmianami relacji między kapitałem własnym a obcym, które wpływają na poziom wyniku finansowego przedsiębiorstwa (Iwaszczuk, 2021). W szerszym kontekście zagadnienia związane z ryzykiem omawiają w swoich publikacjach tacy autorzy, jak: Iwaszczuk (2022), Kowalski (2020), Dzień i Madyda (2019) oraz Kasiewicz i Lepczyński (2013).

W przypadku sieci międzyorganizacyjnych należy zwrócić uwagę na czynniki ryzyka, które mogą wynikać z egzystencji w sformalizowanych przestrzeniach współdziałania partnerów. Według literatury przedmiotu głównym zagrożeniem w tym przypadku jest utrata stabilności sieci, która determinowana jest przede wszystkim:

– nadmiernym uzależnieniem od partnera lub partnerów,
– brakiem zaufania między stronami,
– złożonością i trudnością wspólnie realizowanych procesów,
– nierównym poziomem zdolności nabywania nowych kompetencji i umiejętności (Klimas, 2013).

W ramach kooperacji w sieci organizacje mogą podejmować wspólne decyzje strategiczne, które mają na celu zwiększenie efektywności ich działań, w tym także w walce z czynnikami ryzyka, aby skuteczniej im zapobiegać lub zbudować system reagowania na ewentualne zagrożenia. Czynniki ryzyka stanowią integralną część prowadzenia biznesu. W sieciach międzyorganizacyjnych, które złożone są z wielu partnerów biznesowych, ryzyka te mogą przybrać jeszcze większe rozmiary, ponieważ dotyczą nie tylko samej organizacji, ale także jej partnerów handlowych (Sroka & Cygler, 2014).

Efektywność w sieci definiowana jest jako osiąganie pozytywnych wyników, na poziomie kooperacyjnym sieci, które nie mogłyby być osiągnięte przez poszczególnych uczestników działających niezależnie. Efektywne sieci w literaturze przedmiotu posiadają następujące cechy charakterystyczne:
– Są centralnie zintegrowane.
– Istnieją od co najmniej 3 lat.
– Wykazują wysoki stopień stabilności.
– Dysponują znacznymi zasobami (Popp et al., 2014).

Wspólne podejmowanie decyzji i opracowywanie strategii pozwala partnerom biznesowym na zwiększenie zaangażowania w działania na rzecz sieci międzyorganizacyjnej oraz na poprawę jakości i efektywności tych działań. Dzięki temu organizacje w sieci mogą skuteczniej radzić sobie z potencjalnym ryzykiem oraz zagrożeniami, co przekłada się na zwiększenie ich konkurencyjności i może pozytywnie wpłynąć na wyniki finansowe (Iwaszczuk, 2021). W szerszym ujęciu zagadnienia związane z zarządzaniem ryzykiem w organizacji omawiają w swoich publikacjach tacy autorzy, jak: Morawska i Nikścin (2016), Brdulak (2015), Adam i in. (2015) oraz Staniec (2013).

Metodyka badawcza

Badanie zostało przeprowadzone na podstawie studium przypadku platformy Ariba Network. Do zebrania niezbędnych danych wykorzystano metodę badania dokumentów. Informacje na temat organizacji uczestniczących w sieci oraz platformy Ariba Network zostały pozyskane z raportów spółki SAP, które dostępne są na oficjalnej stronie internetowej przedsiębiorstwa. Analiza danych została przeprowadzona przy wykorzystaniu technik analizy treści, a wyniki zostały przedstawione w formie tabel i rysunków. Wiarygodność i rzetelność badania zostały zapewnione przez dokładne przestrzeganie procedur badawczych oraz wykorzystanie źródeł danych z oficjalnej strony internetowej organizacji SAP.

Celem badania jest zidentyfikowanie i ocena wpływu czynników ryzyka na procesy biznesowe platformy Ariba Network. Przedmiotem badania są potencjalne czynniki ryzyka w sieci międzyorganizacyjnej, opartej na platformie Ariba Network,

DOI: 10.17512/znpcz.2023.2.08

która umożliwia organizacjom optymalizację łańcucha dostaw poprzez ułatwienie procesów wymiany handlowej pomiędzy jednostkami gospodarczymi. Działania przedsiębiorstw, w ramach funkcjonującej platformy, odbywają się na zasadach kooperacji, co świadczy o istnieniu specyficznych relacji pomiędzy organizacjami. Podmiotem badania jest organizacja SAP (jako koordynator platformy) oraz sieć międzyorganizacyjna, oparta na platformie Ariba Network. Badanie skupia się na analizie dostępnych danych, które pochodzą z oficjalnych raportów przedsiębiorstwa SAP oraz dokumentów związanych z działalnością tej platformy.

Ze względu na złożoność analizy konieczne było ustrukturyzowanie podejmowanych działań. W związku z tym badanie zostało podzielone na następujące etapy:

1. Analiza dokumentów udostępnianych przez platformę Ariba Network.
2. Zidentyfikowanie czynników ryzyka w sieci międzyorganizacyjnej.
3. Analiza i ocena wpływu czynników ryzyka na procesy biznesowe platformy Ariba Network.
4. Opracowanie wniosków i rekomendacji.

Do realizacji celu badań sformułowano pytania badawcze, które stanowiły podstawę dla dalszych działań, w tym doboru odpowiednich metod zbierania i analizowania danych. Ponadto precyzyjne określenie pytań badawczych pozwoliło na skoncentrowanie się na aspektach sieci, na które należało zwrócić szczególną uwagę podczas tego badania. W związku z powyższym sformułowano następujące pytania badawcze:

1. Jakie są najważniejsze czynniki ryzyka wpływające na procesy biznesowe platformy Ariba Network?
2. W jaki sposób funkcjonują mechanizmy zarządzania ryzykiem na platformie Ariba Network?

Wypisanie pytań badawczych umożliwia łatwiejszą interpretację wyników badania. Ponadto poszukiwanie odpowiedzi na postawione pytania pozwala ująć szerszy kontekst analizowanych treści.

Wyniki badań

Istota platformy Ariba Network

Ariba Network to platforma e-commerce, która umożliwia przedsiębiorstwom nawiązywanie kontaktów z dostawcami oraz zarządzanie procesami zakupowymi. Platforma oferuje możliwość dokonywania transakcji online, negocjowania warunków handlowych, generowania zamówień oraz realizacji płatności. Ponadto Ariba Network dostarcza narzędzi analitycznych do monitorowania procesów zakupowych, stanów magazynowych oraz raportowania wyników biznesowych (SAP, 2023a). Koordynatorem platformy jest spółka SAP, odpowiedzialna za utrzymanie serwerów systemu oraz wprowadzanie ewentualnych korekt w działaniu aplikacji.

Najważniejszym elementem platformy jest system Enterprise Resource Planning (ERP) – oprogramowanie, które integruje procesy i dane biznesowe w organizacji. System ERP umożliwia zarządzanie kluczowymi obszarami firmy, takimi jak produkcja, magazynowanie, sprzedaż, finanse, kadry czy logistyka, poprzez integrację

wszystkich tych obszarów na jednej platformie. Dzięki temu informacje z poszczególnych działów są dostępne w czasie rzeczywistym, co pozwala na efektywniejsze zarządzanie procesami biznesowymi. System ERP zapewnia integrację procesów w organizacji na szeroką skalę i ułatwia koordynację pracy pomiędzy różnymi działami przedsiębiorstw (SAP, 2023b).

Identyfikacja czynników ryzyka

Według raportu przedsiębiorstwa SAP (2023b) w organizacji wyróżnia się kilka rodzajów czynników ryzyka, które mogą mieć znaczący wpływ zarówno na sieć międzyorganizacyjną, jak i na firmę odpowiedzialną za nadzór i koordynację systemu platformy Ariba Network. Poniżej przedstawiono ogólny i szczegółowy podział czynników ryzyka, które zidentyfikowano w badanej jednostce.

1. Ryzyko ekonomiczne, polityczne, społeczne oraz regulacyjne:
   - Globalne środowisko gospodarcze i polityczne, w tym: ryzyko wystąpienia kryzysu na rynkach kredytowych; ryzyko utraty płynności finansowej wśród podmiotów, z którymi podejmowana jest współpraca na rynku globalnym; ryzyko wystąpienia regionalnych lub globalnych recesji; ryzyko wystąpienia gwałtownych wahań cen towarów, kursów walutowych lub stóp procentowych; ryzyko wysokiej stopy inflacji lub deflacji; występowanie niekorzystnych wydarzeń geopolitycznych; ryzyko wzrostu napięcia militarnego na świecie; ryzyko wystąpienia globalnych chorób pandemicznych.
   - Prawo oraz regulacje międzynarodowe, w tym: zmiany przepisów podatkowych; zmiany standardów sprawozdawczości zewnętrznej; zmiany w interpretacji złożonych przepisów podatkowych w różnych krajach; wprowadzanie nowych koncepcji podatkowych, które stanowią zagrożenie dla zinformatyzowanych modeli biznesu; sprzecznych polityk fiskalnych w różnych krajach; przepisy dotyczące importu oraz eksportu; ryzyko wystąpienia sankcji handlowych.
   - Polityka prywatności i własność intelektualna, w tym: ryzyko wystąpienia zmian prawnych dotyczące naruszenia własności intelektualnej; wprowadzenie regulacji dotyczących korzystania z kodu open source; roszczenia dotyczące naruszenia własności intelektualnej podmiotów wyłączonych z sieci międzyorganizacyjnej.
   - Ochrona danych osobowych oraz polityka prywatności, w tym: złożone przepisy dotyczące ochrony danych osobowych; zróżnicowane podejście w lokalnych przepisach do polityki prywatności; ograniczenia w wymianie informacji wynikające z rozwoju prawnych regulacji dotyczących ochrony danych osobowych; możliwość naruszenia danych organizacji przez cyberataki.
2. Ryzyko związane z ładem korporacyjnym i zgodnością z przepisami:
   - Etyka w biznesie, w tym: nieprzestrzeganie zasad wynikających z przepisów antykorupcyjnych w Niemczech, amerykańskiej ustawy o zagranicznych praktykach korupcyjnych, brytyjskiej ustawy o przekupstwie oraz innych lokalnych przepisów zakazujących zachowań korupcyjnych; ryzyko wystąpienia korupcji wśród członków sieci międzyorganizacyjnej; transakcje w sektorze publicznym na terytoriach narażonych na wysokie ryzyko korupcji.

3. Ryzyko wynikające z działalności operacyjnej:
   - Sprzedaż i usługi, w tym: ryzyko spowodowane niewystarczającymi lub nieprawidłowymi informacjami dostarczanymi przez klientów; niewystarczające zarządzanie oczekiwaniami klientów, w tym zakresem oraz możliwościami integracji w systemie; brak odpowiedniego zaangażowania klientów; wyzwania związane z osiągnięciem bezproblemowej integracji, wystarczającej automatyzacji i dostosowania poziomu świadczenia usług do oczekiwań klientów; nieadekwatne modele kontraktowania i konsumpcji oparte na modelach subskrypcyjnych dla usług, wsparcia i zarządzania aplikacjami w systemie; odstępstwa od standardowych warunków świadczenia usług; oświadczenia dotyczące rozwiązań informatycznych, które mogą być błędnie odebrane przez klientów jako zobowiązania dotyczące przyszłych funkcjonalności oprogramowania.
   - Partnerski ekosystem, w tym: zagrożenia wynikające ze złożoności współpracy uwarunkowanej liczbą partnerów w sieci; nieprzestrzeganie przez partnerów obowiązujących regulacji dotyczących zgodności z założeniami systemu platformy; nieprzestrzeganie przez partnerów warunków umów w krajach objętych embargiem lub państwach wysokiego ryzyka.
   - Operacje w chmurze, w tym: niewystarczające spełnienie oczekiwań klientów w zakresie usług w chmurze; niedobory pojemności centrów danych, które mogą wpłynąć na zdolności firmy SAP do dostarczania i obsługi usług w chmurze; niestabilność lub brak dostępnej infrastruktury do obsługi usług w chmurze; ryzyko wynikające z dostosowania się do zmiennych potrzeb klientów w zakresie usług w chmurze; ryzyko utraty prawa do korzystania ze sprzętu zakupionego lub dzierżawionego od stron trzecich.
   - Cyberbezpieczeństwo, w tym: ryzyko uzyskania nieautoryzowanego dostępu do systemów platformy Ariba Network przez osoby lub organizacje do tego nieupoważnione; ryzyko wystąpienia incydentów związanych z atakami cybernetycznymi; ryzyko wystąpienia problemów w procesie tworzenia kopii zapasowych danych; zagrożenie dla systemu wynikające z działalności szkodliwego oprogramowania.
   - Technologia i produkty, w tym: ryzyko niedostosowania usług lub produktów do lokalnych standardów oraz wymogów; ryzyko wystąpienia wad oferowanych produktów w zakresie platformy Ariba Network, które mogą mieć negatywny wpływ na funkcjonowanie systemu; niezdolność algorytmów w systemie do prawidłowego dostosowania się do zmieniających się okoliczności; niemożność spełnienia oczekiwań klientów dotyczących czasu i jakości w procesie usuwania usterek.
4. Ryzyko strategiczne:
   - Udział w rynku i zyski, w tym: niekorzystne, krótkoterminowe skutki w zakresie przychodów wynikające z rosnącej działalności w chmurze; niechęć klientów i partnerów do migracji danych i adaptacji do chmury; ryzyko powstania strategicznych sojuszy konkurentów; ryzyko wywierania presji cenowej przez konkurentów; niezdolność do osiągania planowanego wzrostu marży w zaplanowanym czasie.

- Fuzje i przejęcia, w tym: ryzyko niepowodzenia podczas integracji nabytych technologii lub rozwiązań; ryzyko nieudanej integracji nabytych podmiotów i ich działalności; niespełnienie potrzeb klientów lub partnerów przejętej organizacji; niepowodzenie we wdrożeniu, przywróceniu lub utrzymaniu kontroli wewnętrznych, kontroli ujawniania informacji oraz procedur i polityk w spółkach przejmowanych; ryzyko wystąpienia znaczących nieoczekiwanych wydatków gotówkowych.
- Innowacyjność, w tym: ryzyko wystąpienia zmiany wymagań klientów oraz partnerów w zakresie wzmocnienia strategii Intelligent Enterprise; ryzyko niepowodzenia strategii produktowej (SAP, 2023b).

Jako system o zasięgu globalnym platforma Ariba Network podlega wpływom wielu czynników zewnętrznych, które są trudne do przewidzenia. Czynniki ryzyka mogą się szybko rozwijać i są poza wpływem i kontrolą organizacji. W zależności od rodzaju ryzyka różne determinanty mogą mieć wpływ na wzrost zagrożenia ze strony czynników ryzyka. W miarę rozszerzania obszaru funkcjonowania sieci na nowe kraje lub rynki ryzyko związane z prawem międzynarodowym oraz regulacjami może się nasilić. Lokalne przepisy prawa odnoszące się do działalności organizacji w sieci mogą być niejasne, podlegają zmianom w czasie i często potrafią być sprzeczne pomiędzy jurysdykcjami. Dotyczy to wielu aspektów prowadzenia działalności, w tym m.in. polityki podatkowej, ochrony danych osobowych lub zarządzania własnością intelektualną.

Organizacja SAP dostosowuje swoją strategię zarządzania ryzykiem do zmieniających się w czasie warunków otoczenia. W 2018 roku spółka wyodrębniła oddzielną kategorię czynników ryzyka, tj. ryzyko finansowe. Do tej klasyfikacji ryzyka należały takie czynniki, jak: warunki sprzedaży i przychodów, płynność finansowa, zastosowanie zasad rachunkowości, wahania kursów walut, stóp procentowych i cen akcji, ubezpieczenia, Venture Capital oraz zmienność cen rynkowych (SAP, 2019). W swoim rocznym raporcie z 2020 roku (SAP, 2021) organizacja uwzględniła kategorię ryzyka dotyczącą kapitału ludzkiego, w którym omówione zostały szczegółowo czynniki wpływające na ryzyko związane z kadrą pracowniczą.

Mechanizmy zarządzania ryzykiem

Organizacja SAP posiada kompleksowe struktury kontroli wewnętrznej i zarządzania ryzykiem, które umożliwiają wczesną identyfikację i analizę ryzyka oraz podjęcie odpowiednich działań zapobiegawczych. Systemy te mają na celu wykrycie potencjalnych zdarzeń, które mogłyby negatywnie wpłynąć na spółkę oraz sieć międzyorganizacyjną. Struktury kontroli wewnętrznej i zarządzania ryzykiem obejmują liczne mechanizmy nadzoru, które są istotnym elementem korporacyjnego procesu decyzyjnego. Są one wdrażane w całej grupie spółek zależnych jako integralna część procesów biznesowych firmy SAP. Organizacja przyjęła zintegrowane podejście do kontroli wewnętrznej i zarządzania ryzykiem, aby pomóc w utrzymaniu odpowiedniego i skutecznego zarządzania ryzykiem globalnym, jednocześnie umożliwiając agregację ryzyka i przejrzyste raportowanie na ten temat (SAP, 2023a).

System identyfikacji i kontroli ryzyka w SAP oparty jest na filarach opublikowanych przez Committee of Sponsoring Organizations of the Treadway Commission (COSO) w raporcie dotyczącym zarządzania ryzykiem w organizacjach. W dokumencie przedstawiono kilka zasad, które zawarte zostały w pięciu podstawowych elementach, tj.:

1. Zarządzanie i kultura: ład organizacyjny wzmacnia znaczenie zarządzania ryzykiem w przedsiębiorstwie. Kultura odnosi się do wartości etycznych, pożądanych zachowań oraz zrozumienia ryzyka w jednostce.
2. Strategia i ustalanie celów: zarządzanie ryzykiem w przedsiębiorstwie, strategia i wyznaczanie celów są narzędziami w procesie planowania strategicznego. W organizacji ustala się prawdopodobieństwo wystąpienia ryzyka, na podstawie którego formułowana jest strategia. Cele biznesowe służą do realizacji strategii, a jednocześnie stanowią podstawę do identyfikacji, oceny i reagowania na ryzyko.
3. Wyniki: ryzyko, które może wpłynąć na zrealizowanie strategii i celów biznesowych musi zostać zidentyfikowane i ocenione. Ryzyko należy uszeregować według kryterium ważności na podstawie prawdopodobieństwa jego wystąpienia. Następnie organizacja dokonuje wyboru reakcji na ryzyko.
4. Przegląd i rewizja: analizując wyniki jednostki, organizacja może dokonać oceny funkcjonowania przyjętej strategii zarządzania ryzykiem, porównując dane z kilku okresów. Następnie przedsiębiorstwo może podjąć decyzję o wprowadzeniu niezbędnych zmian w identyfikacji, kontroli oraz zapobieganiu ryzyku.
5. Informacja, komunikacja i raportowanie: zarządzanie ryzykiem przedsiębiorstwa wymaga ciągłego procesu pozyskiwania i udostępniania niezbędnych informacji, ze źródeł wewnętrznych i zewnętrznych (COSO, 2017).

Spółka SAP wykorzystuje własne oprogramowanie do zarządzania ryzykiem w sieci oraz w swoich spółkach zależnych, tj. program SAP Governance, Risk and Compliance (GRC) napędzany przez system SAP HANA. Narzędzie wykorzystywane jest do wspierania procesu zarządzania w organizacji. Menedżerowie ds. ryzyka są odpowiedzialni za rejestrację i monitorowanie zagrożeń w czasie rzeczywistym za pomocą oprogramowania do zarządzania ryzykiem. Działania te mają służyć zapewnieniu przejrzystości wszystkich znanych kategorii ryzyka występujących w grupie spółek zależnych SAP oraz w sieci opartej na platformie Ariba Network. Informacje pozyskane dzięki oprogramowaniu GRC są agregowane, a następnie wydawane regularnie (co kwartał) w formie raportu, który przekazywany jest do zarządu spółki (SAP, 2023a).

Spółka SAP niektóre z zadań przekazuje do realizacji organizacjom zewnętrznym. Zlecenia dotyczą przede wszystkim takich elementów działalności jednostki, jak: wycena przewidywanych zobowiązań z tytułu świadczeń i akcji, kwartalne obliczenia podatkowe dla większości podmiotów oraz sporządzanie sprawozdań finansowych dla kilku ze spółek zależnych. Przekazywane do realizacji zadania podlegają takim samym rygorystycznym wymogom, jakie obowiązują w przypadku wszystkich wewnętrznie generowanych informacji finansowych (SAP, 2023a). Zlecanie zadań jednostkom zewnętrznym może wpłynąć na minimalizację ryzyka w organizacji poprzez zwiększenie dostępności do specjalistycznych zasobów i wiedzy. Zawsze jednak istnieje ryzyko związane z korzystaniem z usług zewnętrznych jednostek,

dlatego ważne jest, aby organizacje miały opracowane odpowiednie procedury zarządzania tym ryzykiem oraz umowy z jasno zdefiniowanymi wymaganiami i warunkami ich rozwiązania.

Organizacja SAP w corocznym raporcie zawiera szacowaną ocenę ryzyka pod względem prawdopodobieństwa jego wystąpienia, wpływu na działalność jednostki oraz ogólnego poziomu zagrożenia, który odnosi się do konkretnego rodzaju ryzyka. W Tabeli 2 zawarto przegląd głównych czynników ryzyka oraz szczegółowej klasyfikacji potencjalnych zagrożeń. Poszczególne czynniki oceniono pod względem prawdopodobieństwa wystąpienia, wpływu na działalność organizacji oraz partnerów w sieci, a także ogólnego zagrożenia, które jest wynikiem agregacji dwóch poprzedzających wartości.

Tabela 2. Ocena kategorii ryzyka według prawdopodobieństwa ich wystąpienia, wpływu oraz ogólnego zagrożenia dla działalności firmy

Wyszczególnienie	Prawdopodobieństwo wystąpienia[2]	Wpływ[3]	Ocena ogólnego zagrożenia[4]
Ryzyko ekonomiczne, polityczne, społeczne oraz regulacyjne:			
Globalne środowisko gospodarcze i polityczne	Prawdopodobne	Duży	Średnie
Prawo oraz regulacje międzynarodowe	Mało prawdopodobne	Krytyczny	Średnie
Polityka prywatności i własność intelektualna	Prawdopodobne	Duży	Średnie
Ochrona danych osobowych	Prawdopodobne	Duży	Średnie
Ryzyko związane z ładem korporacyjnym i zgodnością z przepisami:			
Etyka w biznesie	Prawdopodobne	Duży	Średnie
Ryzyko wynikające z działalności operacyjnej:			
Sprzedaż i usługi	Mało prawdopodobne	Duży	Średnie
Partnerski ekosystem	Mało prawdopodobne	Duży	Średnie
Operacje w chmurze	Mało prawdopodobne	Duży	Średnie

[2] Prawdopodobieństwo oceniano według pięciostopniowej skali, tj.: znikome (1-19%), mało prawdopodobne (20-39%), prawdopodobne (40-59%), bardzo prawdopodobne (60-79%), prawie pewne (80-99%).

[3] Wpływ oceniano według pięciostopniowej skali, tj.: niewielki (od 0 euro do 25 mln euro), niski (od 25 mln euro do 50 mln euro), umiarkowany (od 50 mln euro do 100 mln euro), duży (od 100 mln euro do 500 mln euro), krytyczny (ponad 500 mln euro).

[4] Stopień zagrożenia oceniano według trzystopniowej skali (po uwzględnieniu zastosowania działań zapobiegających ryzyku), tj.: niskie, średnie, wysokie.

Cyberbezpieczeństwo	Prawdopodobne	Krytyczny	Wysokie
Technologia i produkty	Prawdopodobne	Krytyczny	Wysokie
Ryzyko strategiczne:			
Udział w rynku i zyski	Mało prawdopodobne	Krytyczny	Średnie
Fuzje i przejęcia	Mało prawdopodobne	Duży	Średnie
Innowacyjność	Mało prawdopodobne	Duży	Średnie

Źródło: Opracowanie własne na podstawie (SAP, 2023a)

Według oceny zagrożenia ze strony ryzyka, przeprowadzonej przez spółkę SAP, najważniejszymi czynnikami ryzyka, które w najbliższej przyszłości mogą stanowić wyzwanie dla osiągnięcia założonych celów strategicznych, są: cyberbezpieczeństwo oraz technologia i produkty. SAP dostarcza rozwiązań lub zarządza elementami działalności klientów oraz partnerów w chmurze. Pomimo tego, że organizacja SAP posiada kompletną strategię kontroli i zapobiegania ryzyku, to istnieje duże zagrożenie ze strony złożonego środowiska cybernetycznego. Powaga ryzyka wynikająca z tego obszaru jest zwiększona ze względu na coraz bardziej wyrafinowane i złośliwe globalne praktyki związane z atakami informatycznymi. Organizacja SAP posiada szerokie zasoby środków mających na celu przeciwdziałanie i ograniczanie ryzyka w zakresie czynników technologicznych i produktowych. Nie można jednak wykluczyć, że w przypadku wystąpienia jednego lub więcej niepożądanych incydentów w jednostce skutki mogą być krytyczne zarówno dla organizacji, jak i sieci.

Podsumowanie

W otoczeniu organizacji SAP istnieje wiele zagrożeń, które mogą bardzo negatywnie wpłynąć na stabilność sieci międzyorganizacyjnej, pozycję konkurencyjną, ceny akcji, reputację, markę, przepływy pieniężne lub wyniki finansowe przedsiębiorstwa. Co kwartał wyodrębniony w jednostce zespół dokonuje analizy potencjalnego ryzyka, które może mieć wpływ na działalność firmy. Informacje dotyczące zagrożeń są agregowane, a następnie zamieszczane w corocznym raporcie. W najnowszym dokumencie SAP, dotyczącym czynników ryzyka, wyróżniono cztery główne rodzaje ryzyka, które dzielą się łącznie na trzynaście kategorii.

Spółka SAP jest odpowiedzialna nie tylko za swoje wyniki finansowe, przepływy pieniężne, markę i reputację, ale również za wartości generowane przez spółki zależne, partnerów oraz klientów. W związku z tym organizacja poświęca sporo własnych zasobów w celu identyfikacji, kontroli oraz zapobiegania potencjalnemu ryzyku. W przedsiębiorstwie cyklicznie aktualizowana jest strategia zarządzania ryzykiem, która opiera się pięciu filarach zaproponowanych przez organizację COSO w 2017 roku. Działania kontrolne wspierane są przez oprogramowanie GRC. Narzędzie wykorzystuje się do wspierania procesu zarządzania w organizacji.

Spółka SAP, poza formułowaniem strategii przeciw potencjalnym zagrożeniom na własne potrzeby, oferuje swoim partnerom oraz klientom system zarządzania ryzykiem, który pozwala na lepsze zrozumienie ryzyka w otoczeniu oraz poprawia ogólną przejrzystość łańcucha dostaw użytkowników. Dzięki oferowanym systemom uczestnicy sieci opartej na platformie Ariba Network mogą szybciej reagować na potencjalne problemy będące skutkiem zdarzeń, na które zarówno spółka SAP, jak i jej partnerzy nie mają wpływu.

Pomimo unikalności każdej platformy biznesowej wnioski uzyskane z analizy podejścia SAP do zarządzania ryzykiem mogą być w pewnym stopniu ekstrapolowane na inne organizacje i sieci międzyorganizacyjne. Kluczowe elementy, takie jak regularna identyfikacja, kontrola i przeciwdziałanie zagrożeniom, a także ciągłe dostosowywanie strategii zarządzania ryzykiem do obserwacji otoczenia, są uniwersalne i mogą być stosowane przez wiele przedsiębiorstw, niezależnie od branży czy typu działalności. Dodatkowo oferowanie systemów zarządzania ryzykiem dla partnerów i klientów, tak jak to robi SAP, może być powszechną praktyką, zwiększającą przejrzystość i reaktywność całego łańcucha dostaw.

Podejście SAP do zarządzania ryzykiem, które obejmuje cykliczną aktualizację strategii w corocznych raportach, jest wartościowym elementem, który mógłby być naśladowany przez inne platformy. W tym kontekście konieczne będzie uwzględnienie unikalnych cech każdej organizacji, w tym jej struktury, kultury i rynku działania. W praktyce, mimo że procesy i systemy SAP mogą służyć jako wzór, istotne jest dostosowanie strategii zarządzania ryzykiem do specyficznych potrzeb i wymagań innych platform. Bez tego spersonalizowanego podejścia ekstrapolacja wyników SAP może nie przynieść oczekiwanych rezultatów.

Literatura

Adamik, A. (Red.) (2021). *Nauka o organizacji. Ujęcie dynamiczne*. Wydawnictwo Nieoczywiste.

Barczak, B. (2020). *Modele sieci organizacyjnych*. Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie.

Bergenholtz, C., & Waldstrøm, C. (2011). Inter-Organizational Network Studies – A Literature Reviev. *Industry and Innowation*, *18*(6), 539-562. DOI:10.1080/13662716.2011.591966

Borkowski, P. (2008). *Ryzyko w działalności przedsiębiorstw*. Wydawnictwo Uniwersytetu Gdańskiego.

Brdulak, J. (2015). *Zarządzanie ryzykiem i zmianami w organizacji*. Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej w Lublinie.

COSO. (2017). *Enterprise Risk Management – Integrating with Strategy and Performance*. https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf (dostęp: 25.04.2023).

Dzień, M., & Madyda, A. (2019). *Etyka i ryzyko w biznesie: wybrane zagadnienia*. Wydawnictwo Akademii Techniczno-Humanistycznej w Bielsku-Białej.

Hejduk, I. (2014). *Relacje międzyorganizacyjne w naukach o zarządzaniu*. Wolters Kluwer. https://www.sap.com/poland/products/spend-management/ariba-network.html (dostęp: 05.06.2023).

Iwaszczuk, N. (2021). *Ryzyko w działalności gospodarczej: definicje, klasyfikacje, zarządzanie*. Wydawnictwo IGSMiE PAN.

Iwaszczuk, N. (2022). *Przedsiębiorczość i ryzyko w działalności gospodarczej*. Wydawnictwo Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie.

Kasiewicz, S., & Lepczyński, B. (2013). *Ryzyko w zarządzaniu strategicznym. Natura i uwarunkowania*. Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.

Klimas, P. (2013). Uwarunkowania skutecznej współpracy międzyorganizacyjnej. *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, *141*, 185-198. https://www.sbc.org.pl/dlibra/publication/edition/82387?id=82387&from=publication (dostęp: 25.04.2023).

Kotłowska, M. (2016). Obszary ryzyka prowadzenia działalności przedsiębiorstw ciepłowniczych. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, *440*, 317-326. DOI: 10.15611/pn.2016.440.30

Kowalski, T. (2020). *Zarządzanie w organizacji*. Wydawnictwo Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy.

Krechowicz, M., & Kiliańska, K. (2019). *Relacje międzyorganizacyjne w wybranych obszarach*. Wydawnictwo Politechniki Świętokrzyskiej.

Morawska, S., & Nikścin, J. (2016). *Zarządzanie ryzykiem i wartością organizacji – współczesne wyzwania*. Wydawnictwo Uniwersytetu Gdańskiego.

Niemczyk, J., Jasiński, B., & Stańczyk-Hugiet, E. (2012). *Sieci międzyorganizacyjne. Współczesne wyzwanie dla teorii i praktyki zarządzania*. C.H. Beck.

Oliński, M. (2019). *Model biznesu sieci przedsiębiorstw: budowa, identyfikacja, ocena*. Wydawnictwo Naukowe PWN.

Popp, J. K., Milward, H. B., MacKean, G., Casebeer, A., & Lindstrom, R. (2014). *Inter-Organizational Networks. A Reviev of the Literature to Inform Practice*. Wydawnictwo IBM Center for The Business of Government.

Raab, J. (2018). Interorganizational Networks. W: R. Alhajj, J. Rokne (Eds.). *Encyclopedia of Social Network Analysis and Mining* (1035-1060). Springer. DOI: 10.1007/978-1-4939-7131-2_369

SAP. (2019). *SAP Annual Report on Form 20-F 2018*. https://www.sap.com/docs/download/investors/2018/sap-2018-annual-report-form-20f.pdf (dostęp: 22.04.2023).

SAP. (2021). *SAP Annual Report on Form 20-F 2020*. https://www.sap.com/integrated-reports/2020/en.html?pdf-asset=66dcdffb-d17d-0010-87a3-c30de2ffd8ff&page=1 (dostęp: 21.04.2023).

SAP. (2023a). *SAP Annual Report on Form 20-F 2022*. https://www.sap.com/integrated-reports/2022/en.html?pdf-asset=26fe5791-647e-0010-bca6-c68f7e60039b&page=1 (dostęp: 21.04.2023).

SAP. (2023b). *SAP Integrated Report 2022*. https://www.sap.com/integrated-reports/2022/en.html?pdf-asset=8230868e-647e-0010-bca6-c68f7e60039b&page=1 (dostęp: 20.04.2023).

Skrzypek, E. (Red.). (2015). *Zarządzanie ryzykiem i zmianami w organizacji*. Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej w Lublinie.

Sroka, W., & Cygler, J. (2014). Pathologies in Inter-Organizational Networks. *Procedia Economics and Finance*, *12*, 626-635. DOI: 10.1016/S2212-5671(14)00387-6

Staniec, I. (2013). Zarządzanie ryzykiem w organizacji w świetle paradygmatu sieciowego. *Organizacja i Zarządzanie*, *3*(23), 147-157. https://oamquarterly.polsl.pl/wp-content/uploads/2018/01/10-Staniec-KN23.pdf (dostęp: 08.05.2023).

Światowiec-Szczepańska, J. (2016). Tworzenie i zawłaszczanie wartości na rynku B2B. *Handel Wewnętrzny*, *4*(363), 313-324. http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-68a5843b-5231-4d10-a25b-a0d6e0728d46 (dostęp: 24.04.2023).

Wasiluk, A., & Tomaszuk, A. (2020). *Organizacja w sieci relacji*. Wydawnictwo Politechniki Białostockiej.

Wkład autorów: 100% – Kacper Sieciński.

Konflikt interesów: Brak konfliktu interesów.

Źródło finansowania: Brak finansowania.

INTER-ORGANIZATIONAL NETWORK IN THE FACE OF RISK FACTORS: CASE STUDY OF ARIBA NETWORK PLATFORM

Abstract: Inter-organizational networks in the business to business (B2B) model are characterized by a large number of participants, which entails a number of risk factors that may affect business processes in these networks. Therefore, it is important to thoroughly examine these determinants and develop appropriate strategies to minimize risks. The aim of this study is to identify risk factors in the inter-organizational network operating within the Ariba Network platform, and to assess the impact of these elements on business processes in this network. As part of the study, the mechanisms for minimizing threats used in the studied entity were analyzed, as well as the tools utilized to enhance the security of the processes taking place in the network. The practice of counteracting internal and external threats in the studied platform is based on distinguishing four main categories of potential threats. The ability to identify and forecast the probability of the occurrence of risks may prove crucial to maintaining the stability of business processes. Organizations using the resources of the Ariba Network platform are monitored, and the acquired information is processed to develop future threat prevention strategies. The knowledge gained as a consequence of the study may prove useful for companies that operate in the B2B business model, and want to minimize the risks arising from irregularities in cooperation between members of the inter-organizational network.

Keywords: business to business (B2B), risk factors, e-commerce, inter-organizational networks