Ujawnienia w obszarze ryzyka operacyjnego (informacja wynikająca z Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach - Rekomendacja 17)

Suma strat brutto z tytułu ryzyka operacyjnego odnotowanych w 2025 roku, w podziale na klasy zdarzeń i kategorie zdarzeń w ramach rodzajów zdarzeń, przedstawia się następująco:

	Klasy zdarzeń	Kategorie zdarzeń w ramach rodzajów zdarzeń	Suma strat brutto (potencjalnych i rzeczywistych) z tytułu ryzyka operacyjnego odnotowanych w 2025 roku *w tys. zł*	Ilość zdarzeń (wszystkich)
I	Oszustwa wewnętrzne	1. Działania nieuprawnione	0,00	0
		2. Kradzież i oszustwo	0,00	0
II	Oszustwa zewnętrzne	1. Kradzież i oszustwo	0,00	12
		2. Bezpieczeństwo systemów	0,00	615
III	Zasady dotyczące zatrudnienia oraz bezpieczeństwo w miejscu pracy	1. Stosunki pracownicze	57,13	45
		2. Bezpieczeństwo środowiska pracy	0,00	0
		3. Podziały i dyskryminacja	0,00	0
IV	Klienci, produkty i normy prowadzenia działalności	1.Obsługa klientów, ujawnianie informacji o klientach, zobowiązania względem klientów	37,19	38
		2. Niewłaściwe praktyki biznesowe lub rynkowe	0,00	0
		3. Wady produktów	0,00	0
		4. Klasyfikacje klienta i ekspozycje	0,00	0
		5. Usługi doradcze	0,00	0
V	Szkody związane z aktywami rzeczowymi	Klęski żywiołowe i inne zdarzenia	0,37	3
VI	Zakłócenie działalności gospodarczej i awarie systemu	Systemy	6,75	53

VII	Wykonanie transakcji, dostawa i zarządzanie procesami	1. Wprowadzanie do systemu, wykonywanie, rozliczanie i obsługa transakcji	3,23	1789
		2. Monitorowanie i sprawozdawczość	0,00	0
		3. Napływ i dokumentacja dotycząca klienta	0,00	0
		4. Zarządzanie rachunkami klientów	0,00	0
		5. Uczestnicy procesów niebędący klientami Banku (np. izby rozliczeniowe)	0,00	0
		6. Sprzedawcy i dostawcy	0,00	0
	RAZEM		**104,67**	**2555**

Alokacja funduszy na ryzyko operacyjne odbywa przy wykorzystaniu miar przekształcania ryzyka w wymogi kapitałowe z tytułu ryzyka operacyjnego określonych w Rozporządzeniu UE 575/2013 z dnia 26 czerwca 2013 r. z późniejszymi zmianami. Bank wylicza wymóg kapitałowy z tytułu ryzyka operacyjnego w oparciu o metodę standardową, o której mowa w art. 312-315 w/w Rozporządzenia UE. Bank posiada wystarczające kapitały na zabezpieczenie ryzyka operacyjnego.

Działania mitygujące podejmowane przez Bank w celu uniknięcia strat w przyszłości oraz ograniczania występowania takich samych lub podobnych zdarzeń to przede wszystkim wdrażanie i systematyczna weryfikacja procesów zapobiegania występowania oraz zmniejszania skutków ryzyka, odpowiednio do rodzaju ryzyka i jego możliwego wpływu na wynik Banku; zapobieganie powstawaniu zagrożeń o charakterze katastroficznym lub zagrażającym utratą ciągłości działania Banku; działania prewencyjne związane z identyfikacją i monitoringiem ryzyka prowadzenia operacji, rozpoznawaniem i zapobieganiem powstawaniu zdarzeń ryzyka operacyjnego w trakcie codziennej działalności a także zapewnienie identyfikacji i oceny ryzyka przed podjęciem istotnych decyzji związanych z wdrożeniem nowych produktów, procesów, systemów; osłabianie i niwelowanie skutków zdarzeń poprzez przygotowanie odpowiednich procedur i sposobów reagowania pracowników Banku na wypadek zajścia zdarzenia ryzyka operacyjnego a także poprzez dokonanie przeniesienia ryzyka na inne podmioty w przypadku opłacalności i dostępności takiej metody dla danego rodzaju ryzyka; stosowanie ubezpieczeń, tworzenie planów awaryjnych zachowania ciągłości działania a także okresowa weryfikacja procedur obowiązujących w Banku, zapewnienie bieżących szkoleń dla pracowników Banku, utrzymywanie infrastruktury teleinformatycznej Banku na wysokim poziomie i zapewnienie odpowiedniego poziomu operacyjnej odporności cyfrowej.

W okresie 2025 roku Bank działał w warunkach dynamicznie zmieniającego się otoczenia zewnętrznego, w tym otoczenia regulacyjnego i gospodarczego. Sytuacja makroekonomiczna oraz geopolityczna przyczyniła się do wzrostu aktywności klientów, urzędów, instytucji nadzorczych oraz samego Banku w przestrzeni cyfrowej. W 2025 roku kluczowym wyzwaniem regulacyjnym i operacyjnym stało się pełne wdrożenie unijnego Rozporządzenia DORA, które nałożyło na Bank rygorystyczne obowiązki w zakresie zarządzania ryzykiem ICT, testowania odporności systemów oraz monitorowania incydentów.

Powyższe czynniki stały się powodem wzrostu znaczenia systemów informatycznych oraz wzrostu ryzyka w obszarze cyberbezpieczeństwa, co przyczyniło się bezpośrednio do zwiększenia ryzyka ICT w działalności Banku.

Na przestrzeni 2025 roku nie wystąpiły żadne zdarzenia, które mogłyby mieć bezpośredni wpływ na zmianę profilu ryzyka i które można określić jako znaczące. W oparciu o analizę rejestru zdarzeń operacyjnych można stwierdzić, że procesy jak i zdarzenia występujące podczas działania Banku były przez Bank znane i zidentyfikowane, w związku z czym można stwierdzić, że są bezpieczne. Proces zarządzania ryzykiem operacyjnym w Banku odbywa się w sposób ciągły.

WICEPREZES ZARZĄDU
Alicja Kubeczko

WICEPREZES ZARZĄDU
Barbara Bracka

PREZES ZARZĄDU
Barbara Frycz