**Polityka Zarządzania Ryzykiem ICT (zgodna z DORA)**

|  |  |
| --- | --- |
| Wersja | v2.0 (zmiany organizacyjne) |
| Data | 2025-10-07 |
| Właściciel | Chief Operating Officer (COO) |
| Jednostka nadzorująca | Zarząd |
| Gremium komitetowe | Komitet Odporności Cyfrowej (KOC) |
| Zakres organizacyjny | Cała Grupa – rozszerzony nadzór na spółki zagraniczne |

# 1. Cel i zakres

Celem Polityki jest ustanowienie jednolitych zasad zarządzania ryzykiem ICT w podmiocie finansowym, zgodnie z Rozporządzeniem (UE) 2022/2554 (DORA) oraz powiązanymi standardami technicznymi (RTS/ITS) i wytycznymi organów nadzoru (EUNB/ESMA/EIOPA). Polityka obejmuje wszystkie procesy, systemy, dane, osoby oraz relacje z dostawcami ICT wpływające na ciągłość krytycznych i istotnych funkcji.

# 2. Definicje

* Ryzyko ICT – ryzyko straty wynikające z nieodpowiedniej lub zawodnej infrastruktury, oprogramowania, osób lub procesów ICT, w tym ryzyka cyber.
* Krytyczna lub istotna funkcja (KIF) – funkcja, której zakłócenie miałoby istotny wpływ na ciągłość działania, klientów lub stabilność finansową.
* Poważny incydent ICT – incydent spełniający progi materialności określone w niniejszej Polityce oraz w przepisach wykonawczych.
* Dostawca ICT – podmiot świadczący usługi, rozwiązania lub zasoby ICT, w tym w modelu chmury.

# 3. Ład organizacyjny i role

Zarząd odpowiada za zatwierdzenie Polityki, wyznacza akceptowalny poziom ryzyka oraz nadzoruje jej wdrożenie. Dyrekcja zapewnia zasoby i egzekwuje stosowanie zasad w jednostkach.

## 3.1 Właściciel Polityki

* Właścicielem Polityki jest Chief Operating Officer (COO).
* Organizacja pierwszej linii odpowiedzialna za bieżące zarządzanie ryzykiem ICT: Biuro Odporności Cyfrowej (BOD) w Departamencie Operacji i IT.
* Niezależna funkcja ryzyka i zgodności raportuje do Zarządu; 2LoD nadal raportuje niezależnie do Komitetu Audytu i Zarządu.

## 3.2 Komitet

* Ustanawia się Komitet Odporności Cyfrowej (KOC) zbierający się co miesiąc (połączony z Komitetem Ciągłości Działania).
* Zakres: przegląd ryzyka ICT, postępu remediacji, wskaźników KRI/KPI, istotnych projektów zmian, akceptacji wyjątków.

## 3.3 Odpowiedzialności kluczowe

* Właściciele procesów biznesowych – identyfikują i oceniają ryzyka ICT w swoich obszarach.
* IT – wdraża kontrole i zapewnia dostępność oraz bezpieczeństwo rozwiązań ICT.
* Biuro Odporności Cyfrowej (BOD) w Departamencie Operacji i IT – utrzymuje ramy, metodologię, rejestr ryzyk ICT, koordynuje testy odporności.
* Dział bezpieczeństwa – prowadzi zarządzanie incydentami, SOC i cyberobronę.
* Jednostka Zarządzania Dostawcami ICT (JZDICT) w BOD – prowadzi zarządzanie relacjami z dostawcami ICT oraz due diligence.

## 3.4 Rejestr ról (RACI) – wycinek

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Obszar | Właściciel | IT | Bezpieczeństwo | Ryzyko/2LoD | Audyt/3LoD |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Identyfikacja ryzyka | A/R | C | C | C | I |
| Ocena i akceptacja | A | C | C | R | I |
| Zarządzanie incydentami | C | R | A | I | I |
| Dostawcy ICT | C | C | C | I | I |

Uwaga: właścicielem obszaru „Dostawcy ICT” jest Jednostka Zarządzania Dostawcami ICT (JZDICT) w BOD; rejestr umów ICT prowadzi JZDICT (centralny rejestr umów ICT).

# 4. Ramy zarządzania ryzykiem ICT

## 4.1 Identyfikacja i klasyfikacja

* Prowadzi się inwentaryzację zasobów ICT, usług i zależności (w tym łańcucha dostaw).
* Klasyfikuje się funkcje jako krytyczne/istotne na podstawie wpływu na klientów, rynek i zgodność.

## 4.2 Ocena ryzyka

* Ocena na poziomie aktywa/usługi oraz agregacja na poziomie procesu i KIF.
* Skala: Prawdopodobieństwo x Wpływ (finanse, klienci, zgodność, reputacja, dostępność).
* Akceptacja ryzyka zgodnie z apetytami i tolerancjami zatwierdzonymi przez Zarząd.

## 4.3 Kontrole i remediacja

* Standardy kontroli w obszarach: dostępność, ciągłość, cyberbezpieczeństwo, zmiany, konfiguracja, tożsamość, dane.
* Plany remediacji z terminami, właścicielem i mierzalnymi rezultatami.

## 4.4 Incydenty ICT i raportowanie

* Proces reagowania (detekcja → analiza → eskalacja → przywrócenie → post-mortem).
* Klasyfikacja poważnego incydentu (próg): niedostępność KIF > 2h lub wpływ > 5 000 klientów, lub istotny wpływ regulacyjny.
* Zgłoszenia do organów nadzoru oraz klientów zgodnie z przepisami i RTS/ITS; prowadzi się rejestr incydentów ICT.

## 4.5 Ciągłość działania i DR

* Cele odtwarzania: dla płatności i bankowości elektronicznej: RTO ≤ 2h, RPO ≤ 30 min; dla pozostałych KIF: RTO ≤ 4h, RPO ≤ 1h.
* Plany BCP/DRP aktualizowane co najmniej rocznie; testy: techniczne, proceduralne i symulacyjne.

## 4.6 Testy odporności cyfrowej

* Testowanie obejmuje skany, testy penetracyjne, scenariusze katastroficzne oraz TLPT (threat‑led). Częstotliwość TLPT: co 2 lata dla KIF o najwyższej krytyczności; co 3 lata dla pozostałych KIF.
* Zaangażowanie niezależnych testerów oraz nadzór 2LoD; wnioski trafiają do Komitetu.

## 4.7 Zmiany ICT

* Kontrola zmian (CAB), ocena wpływu na KIF, okna serwisowe, plan wycofania.
* Zmiany istotne wymagają zgody Komitetu oraz aktualizacji analizy ryzyka.

## 4.8 Dostawcy i łańcuch dostaw ICT

* Due diligence przed zawarciem umowy; ocena ryzyka koncentracji i lock‑in.
* Obowiązkowe klauzule DORA: prawa audytu, dostęp do danych/obiektów, raportowanie incydentów, lokalizacja i podwykonawcy.
* Centralny Rejestr Umów ICT, ocena krytyczności oraz plany wyjścia (exit plans).

## 4.9 Wskaźniki i raportowanie

* KRI/KPI z progami tolerancji: np. dostępność < 99,7% w miesiącu dla kanałów klienta; MTTR > 2h dla KIF; krytyczne łatki > 7 dni.
* Miesięczne raporty operacyjne, kwartalne raporty dla Zarządu, roczne sprawozdanie zgodności DORA.

## 4.10 Szkolenia i świadomość

* Program szkoleń dla wszystkich pracowników (częstotliwość: co 6 miesięcy dla ról kluczowych; raz w roku dla pozostałych + onboarding); moduły specjalistyczne dla ról technicznych i kadry.

# 5. Dokumentacja, przegląd i doskonalenie

* Polityka przeglądana co najmniej raz na 12 miesięcy lub po istotnym incydencie.
* Wszystkie procedury i standardy powiązane są wersjonowane i przechowywane w repozytorium ładu korporacyjnego.
* Wnioski z inspekcji, audytów i testów są śledzone do zamknięcia (closure).

# 6. Wejście w życie

Polityka wchodzi w życie z dniem zatwierdzenia przez Zarząd.