Raport ryzyka dla Zarządu

Przegląd profilu ryzyka bezpieczeństwa informacji i ICT, dane wejściowe do przeglądu zarządzania

PushSec
Zarządzanie ryzykiem ICT
14 września 2026

Klient	**Demo Industrial Sp. z o.o.**	Wersja / status dokumentu	**0.9 / SZKIC (do uzupełnienia przed wydaniem)**
Klasyfikacja	**Poufne, Demo Industrial Sp. z o.o. / PushSec**	Sektor / profil ryzyka	**Inny**
Data raportu	**14 września 2026**	Przygotował	**Rafał Dobrosielski, PushSec**

WYMAGANE DECYZJE ZARZĄDU Zidentyfikowano 1 ryzyk krytycznych oraz 3 ryzyk wysokich lub krytycznych zgłoszonych do akceptacji bez udokumentowanej decyzji Zarządu. Do czasu podjęcia decyzji organizacja ponosi te ryzyka bez formalnej akceptacji.

SPIS TREŚCI

1. Podstawa i zakres raportu
2. Wskaźniki profilu ryzyka
3. Zmiany od poprzedniego przeglądu
4. Rozkład ryzyka rezydualnego
5. Ryzyka istotne dla Zarządu
6. Koncentracja ryzyka
7. Zgodność z apetytem na ryzyko
8. Skuteczność postępowania z ryzykiem
9. Horyzont działań na najbliższy kwartał
10. Kompletność i jakość rejestru
11. Sygnały z incydentów, usług i łańcucha dostaw
12. Odpowiedzialność organu zarządzającego
13. Decyzje wymagane od Zarządu
M1. Pokrycie wejść przeglądu zarządzania
M2. Metodyka i zastrzeżenia

PRÓBKA, DANE FIKCYJNE

1. Podstawa i zakres raportu

Raport przedstawia stan zarządzania ryzykiem bezpieczeństwa informacji i ICT w organizacji Demo Industrial Sp. z o.o.. Stanowi dane wejściowe do przeglądu zarządzania (kl. 9.3 ISO/IEC 27001:2022) oraz dokumentację wyników procesu szacowania i postępowania z ryzykiem (kl. 6.1.2, 6.1.3 i 8.2 normy, proces wg ISO/IEC 27005:2022). Zakres obejmuje 37 ocenionych scenariuszy ryzyka, 17 pozycji inwentarza aktywów. Dane pochodzą z rejestru ryzyk prowadzonego w narzędziu PushRisk, według stanu na 14 września 2026.

Poprzedni punkt odniesienia: migawka profilu ryzyka z 15.06.2026. Zmiany wskaźników odnoszą się do tej daty.

2. Wskaźniki profilu ryzyka

37
RYZYK W REJESTRZE
bez zmian od poprzedniej migawki

18
KRYTYCZNE I WYSOKIE
-2 od poprzedniej migawki

9.3
ŚREDNI WYNIK REZYDUALNY (SKALA 1 DO 25)
-0.6 od poprzedniej migawki

18
POZA APETYTEM
-6 od poprzedniej migawki

100%
RYZYK Z WYBRANĄ OPCJĄ POSTĘPOWANIA

100%
RYZYK Z WŁAŚCICIELEM

0
PRZETERMINOWANYCH DZIAŁAŃ
-5 od poprzedniej migawki

0
RYZYK PO TERMINIE PRZEGLĄDU

3. Zmiany od poprzedniego przeglądu

1
NOWYCH RYZYK

6
WZROST OCENY

9
SPADEK OCENY

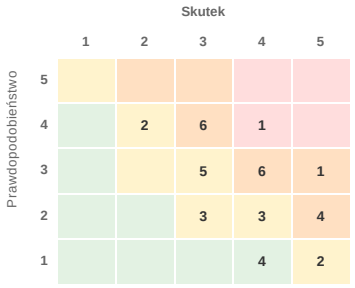
0 / 1
ZAMKNIĘTYCH / USUNIĘTYCH Z REJESTRU

ZMIANA	ID	SCENARIUSZ	POPRZEDNIO	OBECNIE	POZIOM
Nowe	R-001	Phishing masowy prowadzący do kompromitacji konta pracownika	-	**12**	Wysoki
Wzrost	R-006	Były pracownik z nadal aktywnym dostępem do systemów	9	**12**	Wysoki
Wzrost	R-011	Niezadowolony pracownik (insider threat) celowo usuwa lub eksfiltruje dane firmo	7	**10**	Wysoki
Wzrost	R-016	Masowe odejście pracowników IT - utrata wiedzy operacyjnej, niemożność utrzymani	1	**4**	Niski
Wzrost	R-026	Przepełnienie pojemności dyskowej lub pamięci serwera - awaria systemu lub baza	6	**9**	Średni
Wzrost	R-031	Długotrwała przerwa w dostawie energii elektrycznej (>8h) - UPS wyczerpany, gene	1	**4**	Niski

ZMIANA	ID	SCENARIUSZ	POPRZEDNIO	OBECNIE	POZIOM
Wzrost	R-036	Brak przeprowadzenia oceny ryzyka lub nieaktualny rejestr ryzyk - niezgodność IS	5	**8**	Średni
Spadek	R-005	Brak backupu lub backup niedziałający w praktyce	19	**15**	Wysoki
Spadek	R-009	Błąd konfiguracji, publiczny bucket S3 lub storage z danymi	14	**10**	Wysoki
Spadek	R-013	Błąd ludzki administratora: nieintencjonalne usunięcie bazy danych lub konfigura	14	**10**	Wysoki
Spadek	R-017	Sabotaż logiczny przez pracownika - instalacja backdoora lub time-bomby w kodzie	9	**5**	Średni
Spadek	R-021	Brak aktualizacji systemu RODO (RCP, klauzule, DPA) po zmianie procesów przetwar	16	**12**	Wysoki
Spadek	R-025	Awaria dostawcy DNS / CDN - systemy działają, ale są niedostępne z zewnątrz, kli	8	**4**	Niski
Usunięte	R-901	Nieaktualna umowa powierzenia z dostawcą hostingu	12	**-**	-

Pokazano najistotniejsze pozycje w każdej kategorii zmiany. Pełne zestawienie w raporcie Rejestr ryzyk.
Status działań z poprzedniego przeglądu (kl. 9.3.2 a normy): liczba działań zakończonych zmieniła się o -2, co wymaga wyjaśnienia w rejestrze.

4. Rozkład ryzyka rezydualnego



Liczba ryzyk rezydualnych w każdym polu macierzy (prawdopodobieństwo x skutek, skala 1 do 5). Progi poziomów według profilu ryzyka: Niski 1 do 4, Średni 5 do 9, Wysoki 10 do 15, Krytyczny 16 do 25.

POZIOM	LICZBA	UDZIAŁ	ZNACZENIE DECYZYJNE
Krytyczny	1	3%	Natychmiastowe działanie. Akceptacja ryzyka rezydualnego wymaga jawnej, udokumentowanej decyzji Zarządu.
Wysoki	17	46%	Wymaga planu postępowania priorytetowego, raportowanego CISO.
Średni	15	41%	Wymaga planu postępowania w rozsądnym terminie. Monitorowany przez właściciela ryzyka.
Niski	4	11%	Akceptowany bez dodatkowych działań. Przegląd przy następnym cyklu rocznym.

5. Ryzyka istotne dla Zarządu

Ryzyka rezydualne na poziomie Wysokim i Krytycznym, uszeregowane malejąco według wyniku. Kolumna "Redukcja" pokazuje efekt wdrożonych zabezpieczeń: wynik inherentny do rezydualnego.

ID	SCENARIUSZ	KATEGORIA	REDUKCJA	POZIOM	POSTĘPOWANIE	WŁAŚCICIEL	TERMIN	DECYZJA ZARZĄDU
R-003	Nieaktualne oprogramowanie z krytyczną podatnością CVE	Złośliwe działania zewnętrzne	16 → **16**	Krytyczny	Mitygacja	Kierownik Utrzymania Ruchu	*brak terminu*	-
R-005	**Kopie zapasowe (backup)** Brak backupu lub backup niedziałający w praktyce	Złośliwe działania zewnętrzne	15 → **15**	Wysoki	Akceptacja	IT Manager	*nie dotyczy*	**wymagana**
R-001	**Stacje robocze / laptopy pracowników** Phishing masowy prowadzący do kompromitacji konta pracownika	Złośliwe działania zewnętrzne	15 → **12**	Wysoki	Mitygacja	IT Manager	14.10.2026	-
R-002	Brute force lub credential stuffing na konta	Złośliwe działania zewnętrzne	12 → **12**	Wysoki	Mitygacja	Dyrektor techniczny	*brak terminu*	-
R-006	Były pracownik z nadal aktywnym dostępem do systemów	Błędy ludzkie	12 → **12**	Wysoki	Mitygacja	CTO	*brak terminu*	-
R-008	Shadow IT, nieznane systemy z danymi firmowymi	Zdarzenia zewnętrzne	12 → **12**	Wysoki	Mitygacja	CTO	*brak terminu*	-
R-014	**Baza danych klientów (dane osobowe)** Pracownik udostępnia dane klientów nieautoryzowanej osobie trzeciej przez e-mail lub komunikator	Złośliwe działania wewnętrzne	12 → **12**	Wysoki	Mitygacja	DPO	*brak terminu*	-

PRÓBKA, DANE FIKCYJNE

ID	SCENARIUSZ	KATEGORIA	REDUKCJA	POZIOM	POSTĘPOWANIE	WŁAŚCICIEL	TERMIN	DECYZJA ZARZĄDU
R-015	**Stacje robocze / laptopy pracowników** Brak szkoleń z bezpieczeństwa - pracownicy nie rozpoznają phishingu, inżynierii społecznej ani bezpiecznego po	Złośliwe działania wewnętrzne	12 → **12**	Wysoki	Akceptacja	IT Manager	*nie dotyczy*	**wymagana**

6. Koncentracja ryzyka

Gdzie kumuluje się ekspozycja. Koncentracja u jednego właściciela lub w jednym obszarze oznacza, że remediacja zależy od jednego zasobu ludzkiego lub jednej decyzji budżetowej.

WŁAŚCICIEL RYZYKA	RYZYK	W TYM WYSOKIE I KRYTYCZNE	SUMA EKSPOZYCJI
IT Manager	11	5	110
CTO	6	4	56
Kierownik IT	5	3	43
Kierownik Utrzymania Ruchu	6	2	51
DPO	4	2	40
Prokurent ds. operacyjnych	3	1	26

KATEGORIA ZAGROŻENIA	RYZYK	W TYM WYSOKIE I KRYTYCZNE	SUMA
Złośliwe działania wewnętrzne	7	5	63
Złośliwe działania zewnętrzne	5	4	61
Błędy ludzkie	6	4	61
Zdarzenia zewnętrzne	8	3	66
Awarie techniczne	6	1	50
Regulacyjne i prawne	5	1	43

Łańcuch dostaw ICT: 5 ryzyk dotyczy dostawców lub usług zewnętrznych, w tym 1 na poziomie wysokim lub krytycznym. Ryzyko przeniesione do dostawcy pozostaje ryzykiem organizacji.

7. Zgodność z apetytem na ryzyko

18 ryzyk przekracza apetyt zatwierdzony dla swojej kategorii w profilu ryzyka (Profil ogólny). Przekroczenie apetytu wymaga decyzji: obniżyć ryzyko, zmienić apetyt albo formalnie je zaakceptować.

ID	KATEGORIA ZAGROŻENIA	WYNIK REZYDUALNY	APETYT (MAKS.)	PRZEKROCZENIE	POSTĘPOWANIE
R-003	Złośliwe działania zewnętrzne	16	9	+7	Mitygacja
R-005	Złośliwe działania zewnętrzne	15	9	+6	Akceptacja
R-001	Złośliwe działania zewnętrzne	12	9	+3	Mitygacja
R-002	Złośliwe działania zewnętrzne	12	9	+3	Mitygacja
R-006	Błędy ludzkie	12	9	+3	Mitygacja
R-014	Złośliwe działania wewnętrzne	12	9	+3	Mitygacja
R-015	Złośliwe działania wewnętrzne	12	9	+3	Akceptacja
R-018	Błędy ludzkie	12	9	+3	Mitygacja
R-020	Błędy ludzkie	12	9	+3	Akceptacja
R-021	Błędy ludzkie	12	9	+3	Mitygacja
R-027	Awarie techniczne	12	9	+3	Mitygacja
R-033	Regulacyjne i prawne	12	6	+6	Mitygacja

Pokazano 12 pozycji o najwyższym wyniku z 18. Pełna lista w raporcie Rejestr ryzyk.

8. Skuteczność postępowania z ryzykiem

11%
REDUKCJA EKSPOZYCJI DZIĘKI ZABEZPIECZENIOM

0 / 30
DZIAŁAŃ ZAKOŃCZONYCH

8
DZIAŁAŃ W TOKU

7
RYZYK ZAAKCEPTOWANYCH

Redukcja ekspozycji to różnica między sumą wyników inherentnych (387) a rezydualnych (344), czyli deklarowany efekt wdrożonych zabezpieczeń. Wartość wymaga potwierdzenia dowodami skuteczności (audyt wewnętrzny, testy), zanim zostanie uznana za zweryfikowaną.

PRÓBKA, DANE FIKCYJNE

9. Horyzont działań na najbliższy kwartał

Działania z terminem do 13.12.2026. Ta lista jest podstawą do rozliczenia na kolejnym przeglądzie.

TERMIN	ID	DZIAŁANIE	WŁAŚCICIEL	POZIOM RYZYKA	STATUS
14.10.2026	R-001	Wdrożenie zabezpieczenia dla: Phishing masowy prowadzący do kompromitacji konta	IT Manager	Wysoki	W toku
14.10.2026	R-009	Wdrożenie zabezpieczenia dla: Błąd konfiguracji, publiczny bucket S3 lub storage	Kierownik IT	Wysoki	W toku
14.10.2026	R-017	Wdrożenie zabezpieczenia dla: Sabotaż logiczny przez pracownika - instalacja bac	Kierownik IT	Średni	W toku
14.10.2026	R-033	Wdrożenie zabezpieczenia dla: Naruszenie ochrony danych osobowych (wyciek, nieup	IT Manager	Wysoki	W toku
23.11.2026	R-013	Wdrożenie zabezpieczenia dla: Błąd ludzki administratora: nieintencjonalne usuni	Kierownik IT	Wysoki	W toku
23.11.2026	R-021	Wdrożenie zabezpieczenia dla: Brak aktualizacji systemu RODO (RCP, klauzule, DPA	CTO	Wysoki	W toku
23.11.2026	R-029	Wdrożenie zabezpieczenia dla: Kradzież laptopa lub nośnika danych pracownika z d	Kierownik IT	Wysoki	W toku
23.11.2026	R-037	Wdrożenie zabezpieczenia dla: Przetwarzanie danych osobowych poza EOG bez odpowi	Kierownik IT	Średni	W toku

10. Kompletność i jakość rejestru

Poniższe braki ograniczają wiarygodność raportu jako dowodu dla audytora lub organu nadzoru. Ich usunięcie jest zadaniem operacyjnym, nie decyzją Zarządu.

USTALENIE	DLACZEGO TO MA ZNACZENIE
22 działań bez terminu	Działanie bez terminu nie jest planem i nie da się go rozliczyć na kolejnym przeglądzie.
10 aktywów bez przypisanego ryzyka	Aktywa w inwentarzu, dla których nie zidentyfikowano żadnego scenariusza. Wymaga potwierdzenia, że to świadoma decyzja, a nie luka zakresu.

11. Sygnały z incydentów, usług i łańcucha dostaw

Brak sygnałów z modułów incydentów, usług objętych ustawą o KSC i łańcucha dostaw ICT w bieżącym okresie.

12. Odpowiedzialność organu zarządzającego

Odpowiedzialność za system zarządzania bezpieczeństwem informacji spoczywa na najwyższym kierownictwie (kl. 5.1 ISO/IEC 27001:2022) i nie może zostać przeniesiona na zespół operacyjny ani dostawcę. Przyjęcie tego raportu jest wykonaniem obowiązku przeglądu z kl. 9.3.

13. Decyzje wymagane od Zarządu

1 Akceptacja ryzyk wysokich i krytycznych

Do decyzji 3 ryzyk zgłoszonych do akceptacji: R-005, R-015, R-020. Akceptacja ryzyka na tym poziomie wymaga jawnej, imiennej decyzji z uzasadnieniem (kl. 6.1.3 f oraz 8.3 normy).

Decyzja: ..... Osoba: ..... Data: .....

2 Rozstrzygnięcie przekroczeń apetytu

Dla 18 ryzyk poza apetytem Zarząd wskazuje kierunek: dodatkowe zabezpieczenia, zmiana zatwierdzonego apetytu albo świadoma akceptacja przekroczenia.

Decyzja: ..... Osoba: ..... Data: .....

3 Zasoby na uzupełnienie rejestru

Wskazanie osób i czasu na usunięcie braków z sekcji 7. Bez tego kolejny raport będzie obarczony tym samym ograniczeniem.

Decyzja: ..... Osoba: ..... Data: .....

4 Zatwierdzenie raportu jako danych wejściowych do przeglądu zarządzania

Potwierdzenie, że przedstawiony profil ryzyka jest znany Zarządowi i stanowi podstawę decyzji o zasobach na kolejny okres (kl. 9.3 normy).

Decyzja: ..... Osoba: ..... Data: .....

M1. Pokrycie wejść przeglądu zarządzania (kl. 9.3.2)

Raport pokrywa część wymaganych wejść przeglądu zarządzania. Pozostałe elementy muszą być dostarczone z innych źródeł, żeby protokół przeglądu był kompletny wobec normy.

PRÓBKA, DANE FIKCYJNE

WYMAGANE WEJŚCIE	POKRYCIE	ŹRÓDŁO LUB UZUPEŁNIENIE
a) status działań z poprzednich przeglądów	Częściowo	Sekcja 3 pokazuje działania zakończone od poprzedniej migawki. Decyzje Zarządu spoza rejestru ryzyk dostarcza protokół poprzedniego przeglądu.
b) zmiany w czynnikach zewnętrznych i wewnętrznych	Częściowo	Sekcja 3 i 8: nowe ryzyka, zmiany ocen, sygnały z incydentów i łańcucha dostaw. Zmiany organizacyjne, prawne i rynkowe poza rejestrem opisuje kierownictwo.
c) zmiany potrzeb i oczekiwań stron zainteresowanych	Poza raportem	Wymagania klientów, regulatora i partnerów. Źródło: rejestr wymagań stron zainteresowanych (kl. 4.2).
d) informacje zwrotne o działaniu SZBI: niezgodności, monitorowanie, audyty, realizacja celów	Poza raportem	Źródła: raport z audytu wewnętrznego (9.2), rejestr niezgodności (10.2), pomiary z kl. 9.1, rejestr celów (6.2).
e) informacje zwrotne od stron zainteresowanych	Poza raportem	Skargi, wyniki kwestionariuszy bezpieczeństwa klientów, ustalenia audytów klienckich.
f) wyniki oceny ryzyka i status planu postępowania z ryzykiem	Pełne	Sekcje 2 do 9 niniejszego raportu.
g) możliwości ciągłego doskonalenia	Częściowo	Sekcje 10 i 13 wskazują braki i decyzje. Pozostałe źródła doskonalenia poza rejestrem ryzyk.

M2. Metodyka i zastrzeżenia

Proces. Szacowanie i postępowanie z ryzykiem prowadzone zgodnie z ISO/IEC 27005:2022, w powiązaniu z wymaganiami kl. 6.1.2, 6.1.3, 8.2 i 8.3 ISO/IEC 27001:2022. Ocena scenariuszowa: dla każdego scenariusza ustalane są prawdopodobieństwo i skutek w skali 1 do 5, wynik jest ich iloczynem (1 do 25).
Ryzyko inherentne i rezydualne. Inherentne opisuje ekspozycję bez uwzględnienia zabezpieczeń, rezydualne po ich uwzględnieniu. Redukcja jest deklarowana przez właściciela ryzyka i wymaga potwierdzenia dowodami skuteczności zabezpieczeń.
Progi i apetyt. Progi poziomów oraz apetyt per kategoria zagrożenia pochodzą z profilu ryzyka zatwierdzonego dla organizacji (Profil ogólny). Zmiana progów lub apetytu jest decyzją Zarządu, nie zespołu operacyjnego.
Ograniczenia. Raport odzwierciedla wyłącznie scenariusze wprowadzone do rejestru według stanu na 14 września 2026. Nie jest audytem ani niezależną weryfikacją skuteczności zabezpieczeń. Porównania odnoszą się do migawki z 15.06.2026.

Opracował: Rafał Dobrosielski, PushSec
Data: 14 września 2026

Przyjął w imieniu Zarządu:
Imię, nazwisko, data i podpis

PRÓBKA, DANE FIKCYJNE

Próbka dokumentu PushSec. Demo Industrial Sp. z o.o. jest organizacją fikcyjną; wszystkie dane są zmyślone. pushsec.pl