mSecure

CYBERBEZPIECZEŃSTWO | AUDYT | HARDENING

WZORZEC PUBLICZNY / DANE SYNTETYCZNE

MACIERZ GOTOWOŚCI NIS2 / UKSC

Od wymagania i odpowiedzialności do dowodu, luki, ryzyka oraz działania naprawczego

Wykonawca	MSecure Michał Matuszczyk
Organizacja	Jednostka przykładowa
Zakres	Zarządzanie ryzykiem, incydenty, ciągłość, dostawcy, nadzór
Data / wersja	30 sierpnia 2026 / 3.0
Klasyfikacja	PUBLICZNY WZORZEC

Dokument demonstracyjny. Wszystkie parametry środowiska i ustalenia są syntetyczne. Materiał nie zawiera danych żadnego klienta MSecure.

SEKCJA 01

Jak korzystać z macierzy

Macierz nie jest checklistą typu „tak/nie”. Łączy wymaganie z właścicielem procesu, dowodem skuteczności, oceną luki, ryzykiem i konkretnym działaniem. Status bez dowodu ma ograniczoną wartość.

26	8	5	90 dni
obszarów kontrolnych	próbek pokazanych	rodzajów dowodu	pierwsza roadmapa

Status	Znaczenie	Minimalny dowód
Spełnione	Kontrola działa i jest cyklicznie utrzymywana	Konfiguracja/protokół + właściciel + aktualność
Częściowe	Kontrola istnieje, ale zakres lub skuteczność są ograniczone	Dowód istniejący + opisana luka
Niespełnione	Brak kontroli albo brak możliwości wykazania działania	Plan działania i decyzja ryzyka
Nie dotyczy	Wyłączenie uzasadnione zakresem organizacji	Udokumentowane uzasadnienie i zatwierdzenie

SEKCJA 02

Przykładowa macierz zarządcza

ID	Obszar	Oczekiwana kontrola	Właściciel	Dowód	Status	Luka / ryzyko	Działanie
GOV-01	Nadzór	Kierownictwo zatwierdza politykę, ryzyko i program	Zarząd	Protokół + raport kwartalny	Częściowe	Brak cyklicznej informacji o wyjątkach	Włączyć dashboard ryzyka i decyzji
RISK-02	Ryzyko	Metoda, rejestr i właściciele ryzyka	CISO	Metodyka + rejestr + przegląd	Spełnione	Metoda działa; poprawić powiązanie z aktywami	Dodać identyfikatory aktywów i usł
INC-03	Incydenty	Klasyfikacja, eskalacja, zgłaszanie i lessons learned	CSIRT	Procedura + próbka ticketów + ćwiczenie	Częściowe	Brak mierzonego czasu kwalifikacji	Ustalić SLA i przeprowadzić ćwiczen
BCM-04	Ciągłość	BIA, plany, RPO/RTO i testy odtworzenia	BCM / IT	BIA + plan + protokół testu	Niespełnione	RPO/RTO deklarowane, lecz niezmierzone	Test dwóch usług krytycznych i działania
SUP-05	Dostawcy	Ocena przed zakupem, umowy i monitoring	Zakupy	Kwestionariusz + umowa + review	Częściowe	Brak segmentacji dostawców wg krytyczności	Klasyfikacja i minimalne klauzule
IAM-06	Dostęp	Joiner-mover-leaver, MFA, role, recertyfikacja	IAM	Eksport + próbka + access review	Częściowe	Brak cyklicznej recertyfikacji ról	Kwartalny review ról uprzywilejowanych
VUL-07	Podatności	Skanowanie, SLA, wyjątki i walidacja	IT Ops	Raport + ticket + test poprawki	Częściowe	Wyjątki nie mają terminu wygaśnięcia	Rejestr wyjątków z akceptacją ryzy
TRN-08	Świadomość	Program roczny i szkolenie kierownictwa	HR / CISO	Plan + frekwencja + test	Spełnione	Utrzymać; dodać moduł dla zakupów	Rozszerzyć zakres łańcucha dostaw

SEKCJA 03

Karta wymagania - przykład

BCM-04 | Ciągłość działania i odtwarzanie

Pole	Treść
Cel kontrolny	Organizacja rozumie wpływ przerwy, ma zatwierdzone priorytety, osiągalne RPO/RTO i potwierdza je testami.
Stan	Plany istnieją, ale wartości RPO/RTO nie zostały zmierzone dla dwóch usług krytycznych.
Dowód	BIA v2.1, plan DR, konfiguracja backupu, brak protokołu pełnego testu w ostatnich 12 miesiącach.
Ryzyko	Kierownictwo może podejmować decyzje na podstawie celów, których środowisko nie potrafi osiągnąć.
Działanie	Przeprowadzić test odtworzenia, zmierzyć wyniki, porównać z BIA i przypisać działania korygujące.
Kryterium odbioru	Protokół zawiera zakres, czas, wynik, odstępstwa, ownerów i termin retestu; kierownictwo akceptuje ryzyko rezydualne.

Rejestr dowodów

ID	Dokument / źródło	Właściciel	Aktualność	Ocena
E-BCM-01	Analiza wpływu biznesowego v2.1	BCM	2026-Q2	Aktualna
E-BCM-02	Plan odtworzenia usług	IT Ops	2025-Q4	Wymaga aktualizacji
E-BCM-03	Konfiguracja kopii i retencji	Backup Owner	T0	Potwierdzona
E-BCM-04	Protokół testu end-to-end	BCM / IT	Brak	Luka dowodowa

SEKCJA 04

Roadmapa i raportowanie do kierownictwa

Horyzont	Priorytet	Rezultat	Miernik
0-30 dni	Incydenty, role, raportowanie zarządcze	SLA kwalifikacji, review ról, dashboard ryzyka	100% ról z ownerem; próbne zgłoszenie w czasie
31-60 dni	Ciągłość, dostawcy, wyjątki podatności	Test DR, segmentacja dostawców, rejestr wyjątków	Zmierzony RPO/RTO; 100% krytycznych dostawców
61-90 dni	Walidacja i cykl nadzoru	Retesty, aktualizacja ryzyka, przegląd kierownictwa	Dowody zamknięcia albo formalne akceptacje

Minimalny dashboard kwartalny

- liczba ryzyk wysokich i trend;
- status zdolności zgłaszania incydentów oraz wyniki ćwiczeń;
- pokrycie usług krytycznych BIA, planem i zmierzonym RPO/RTO;
- dostawcy krytyczni po ocenie i z wymaganymi klauzulami;
- ustalenia przeterminowane, wyjątki i decyzje wymagane od kierownictwa.

SEKCJA 05

Ograniczenia i zasady bezpiecznego użycia

Wzorzec nie rozstrzyga statusu prawnego żadnej organizacji i nie zastępuje analizy prawnej. Aktualne obowiązki trzeba ustalać na podstawie właściwych przepisów, sektora, rodzaju usług i indywidualnych okoliczności.

Dane syntetyczne

Nazwy, statusy, terminy i dowody w tym dokumencie są przykładowe. Celem jest pokazanie sposobu prowadzenia oceny i raportowania, nie deklaracja zgodności żadnego podmiotu.

W projekcie klient otrzymuje kompletną macierz, repozytorium dowodów, mapę odpowiedzialności, warsztat dla kierownictwa i plan wdrożenia z kryteriami odbioru.

msecure.com.pl | biuro@msecure.com.pl | +48 502 475 670