
# DOBRE PRAKTYKI: DYREKTYWA NIS 2.0 I USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA WHITE PAPER

www.itgrc.pl

BW advisory
Przez naszą wiedzę do Twojej wartości.

01.

# INFORMACJE KONTAKOWE


**Adres:** BW Advisory Sp. z o.o.
ul. Boczańska 25
03-156 Warszawa

**NIP:** 5252818352

**Email:** biuro@itgrc.pl

**Tel.:** +48 604 559 818
+48 603 692 276

**LinkedIn:** www.linkedin.com/company/73523248

02.

# WPROWADZENIE

## Cel i Zakres Dokumentu

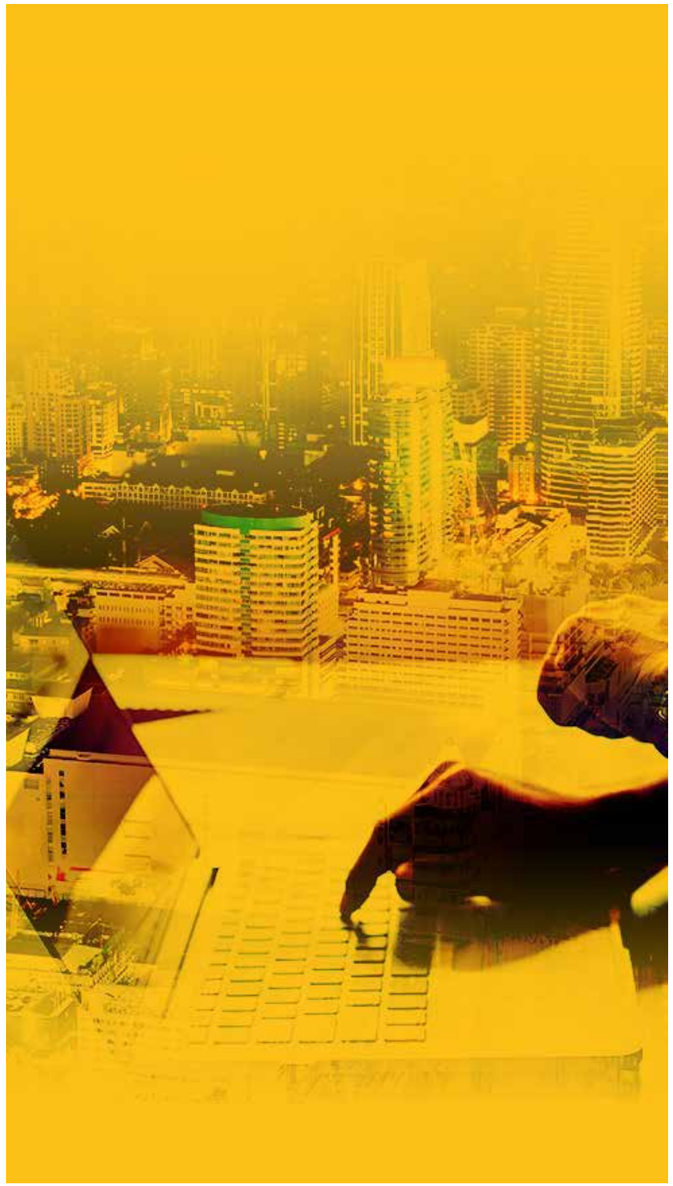
Celem niniejszego dokumentu jest przedstawienie kluczowych informacji dotyczących Dyrektywy NIS 2.0 oraz Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC). Dokument ten ma pomóc przedsiębiorstwom zrozumieć i wdrożyć nowe przepisy dotyczące cyberbezpieczeństwa, które mają na celu podniesienie poziomu bezpieczeństwa w całej Unii Europejskiej, a tym samym w Polsce.

## Znaczenie Cyberbezpieczeństwa w Kontekście NIS 2.0

Cyberbezpieczeństwo stało się jednym z najważniejszych wyzwań dla współczesnych przedsiębiorstw. W dobie rosnącej liczby i zaawansowania ataków cybernetycznych, zarówno na poziomie krajowym, jak i międzynarodowym, konieczne było wprowadzenie spójnych i skutecznych środków ochrony. Dyrektywa NIS 2.0 (Network and Information Security) została opracowana, aby zmodernizować i rozszerzyć zakres poprzednich regulacji (NIS), zapewniając wyższy poziom ochrony dla kluczowych sektorów gospodarki.

## Ogólne Założenia i Cele NIS 2.0

Dyrektywa NIS 2.0, która weszła w życie 16 stycznia 2023 roku, jest kontynuacją wcześniejszych regulacji NIS, mających na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej.



# NOWOŚCI W PORÓWNANIU DO NIS

**W porównaniu do wcześniejszej dyrektywy, NIS 2.0 wprowadza kilka istotnych zmian:**

- Zwiększenie liczby sektorów objętych regulacjami, w tym zdrowia, transportu, przemysłu i usług cyfrowych.
- Terytorialność: Obejmuje podmioty świadczące usługi w UE, nawet jeśli nie mają swojego przedstawicielstwa w UE.
- Zmiana klasyfikacji podmiotów na "istotne" i "ważne", co wiąże się z różnymi wymaganiami dotyczącymi nadzoru i raportowania.
- Wprowadzenie bardziej rygorystycznych wymagań dotyczących zarządzania ryzykiem cyberbezpieczeństwa, w tym łańcucha dostaw oraz zgłaszania incydentów.

# KLUCZOWE DEFINICJE I POJĘCIA

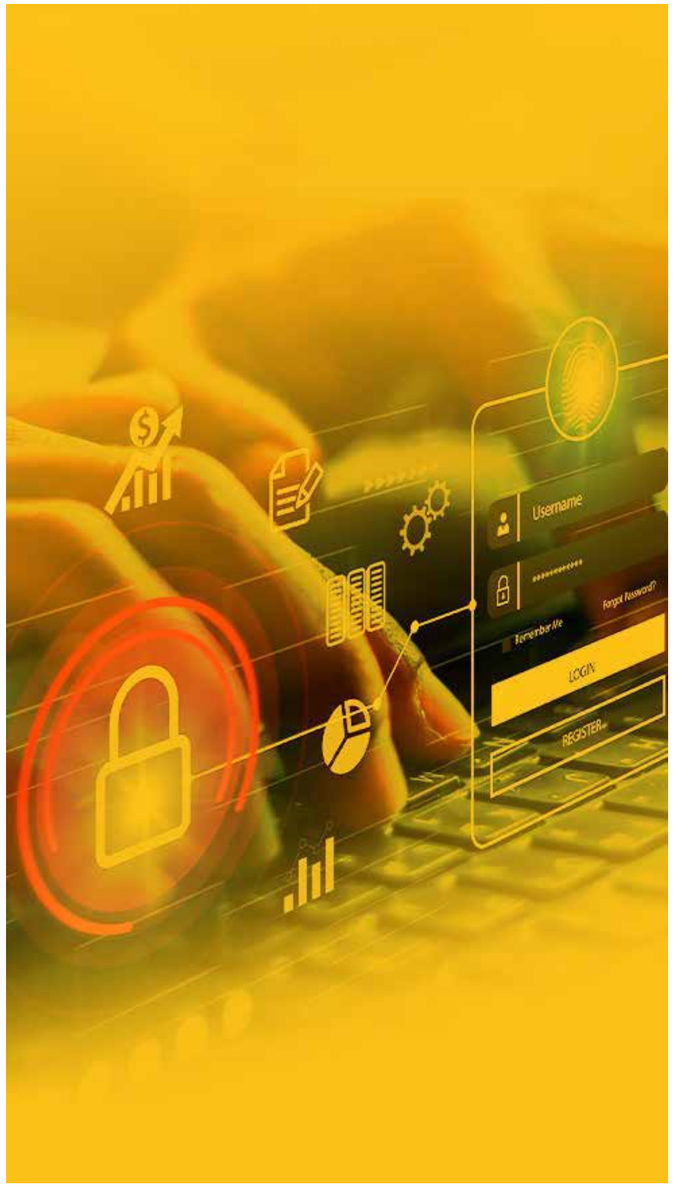
**Podmioty Istotne** – Duże przedsiębiorstwa i organizacje o znaczeniu krytycznym dla gospodarki i społeczeństwa, które są objęte bardziej rygorystycznymi wymaganiami nadzoru.

**Podmioty Ważne** – Mniejsze podmioty, które również mają obowiązek przestrzegania zasad NIS 2.0, ale podlegają mniej surowym wymaganiom nadzoru.

**Dostawcy Usług Komunikacyjnych** – Wskazuje na publicznych dostawców sieci łączności elektronicznej oraz dostawców usług łączności elektronicznej dostępnych publicznie.

**Dostawcy Usług Zaufania i DNS** – Obejmuje dostawców usług zaufania oraz rejestry nazw domen najwyższego poziomu i dostawców usług systemów nazw domen.

**Incydent Cyberbezpieczeństwa** – Każde zdarzenie mające negatywny wpływ na bezpieczeństwo sieci i systemów informatycznych.




# ZMIANY W UKCS

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UKSC) została zaktualizowana w celu harmonizacji z Dyrektywą NIS 2.0, wprowadzając dodatkowe wymagania dla polskich przedsiębiorstw.

# IMPLEMENTACJA I PRAKTYCZNE WSKAZÓWKI

Przygotowanie organizacji do wdrożenia NIS 2.0 i zaktualizowanej UKSC wymaga przeprowadzenia audytu luki obecnych systemów bezpieczeństwa, identyfikacji potencjalnych zagrożeń oraz wdrożenia odpowiednich środków ochrony.

Kluczowe kroki wdrożenia NIS 2.0 obejmują:

- Analizę ryzyka
- Wdrożenie polityk i procedur bezpieczeństwa systemów informatycznych.
- Utworzenie planów ciągłości działania i zarządzania incydentami.
- Wdrożenie mechanizmów technicznych i organizacyjnych ograniczających ryzyka.
- Regularne szkolenia z zakresu cyberbezpieczeństwa dla pracowników.

Niniejszy dokument ma służyć jako przewodnik po najważniejszych aspektach NIS 2.0 i UKSC, pomagając przedsiębiorstwom dostosować się do nowych wymogów i podnieść poziom ochrony swoich zasobów cyfrowych.

03.

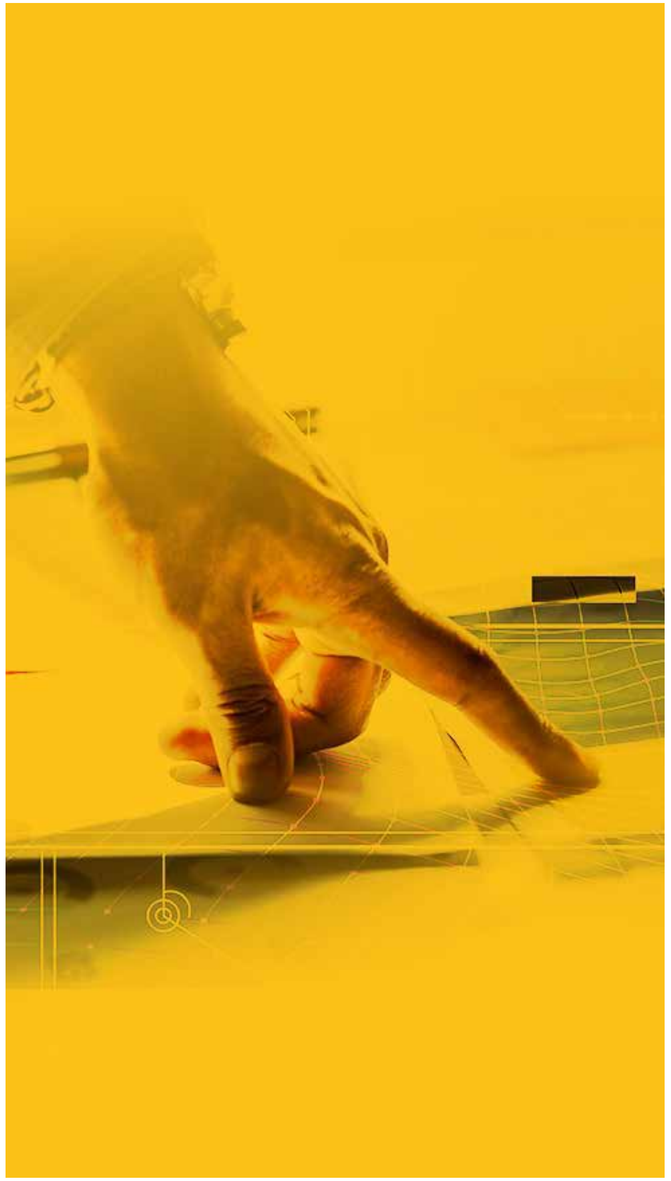
# DYREKTYWA NIS 2.0

## OGÓLNE ZAŁOŻENIA I CELE

Dyrektywa NIS 2.0, przyjęta 16 stycznia 2023 roku, została opracowana, aby zaktualizować istniejące ramy prawne w zakresie cyberbezpieczeństwa i dostosować je do współczesnych wyzwań związanych z rosnącą cyfryzacją oraz ewoluującym krajobrazem zagrożeń cybernetycznych.

**Główne cele dyrektywy obejmują:**

- Rozszerzenie zakresu podmiotów objętych regulacjami, w tym średnich i dużych przedsiębiorstw z różnych sektorów.
- Zwiększenie odpowiedzialności zarządów przedsiębiorstw za cyberbezpieczeństwo.
- Wprowadzenie surowszych kar za nieprzestrzeganie przepisów.
- Ujednolicenie standardów i praktyk cyberbezpieczeństwa w całej UE.



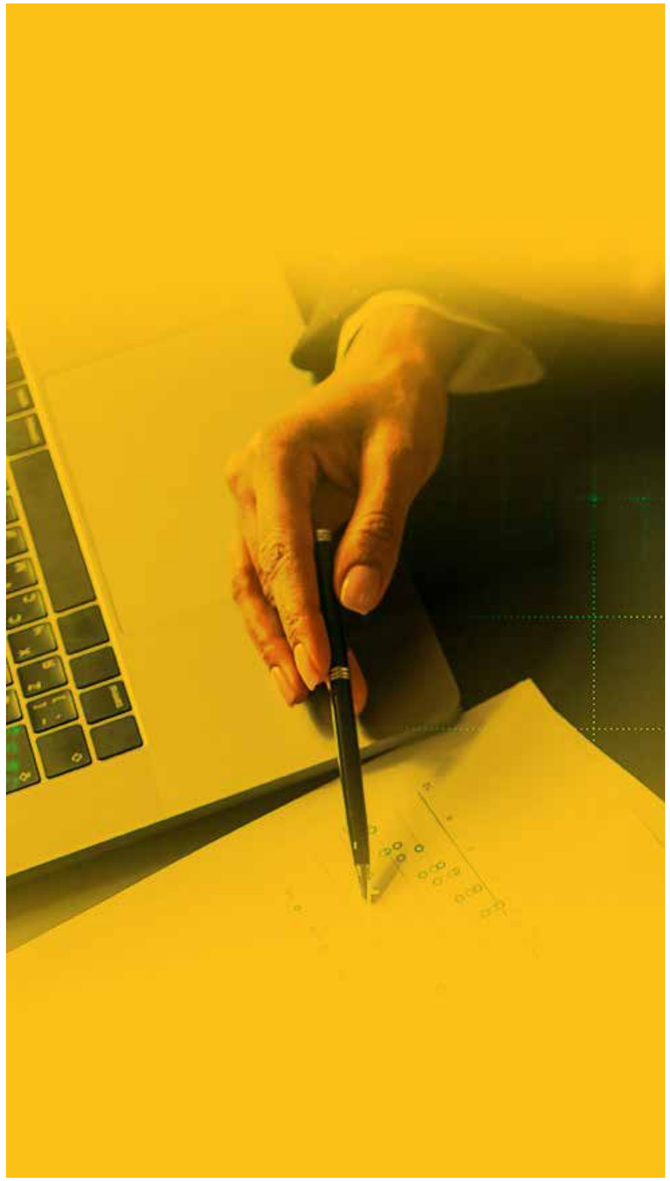
# ZAKRES I ZASTOSOWANIE NIS 2.0

Dyrektywa NIS 2.0 znacząco rozszerza zakres sektorów i podmiotów objętych regulacjami w porównaniu do poprzedniej dyrektywy NIS. Nowe przepisy obejmują zarówno sektory kluczowe, jak i ważne, w tym:

- **Sektory Kluczowe:** energia, transport, bankowość, infrastruktura rynku finansowego, zdrowie, woda pitna, odpady wodne, infrastruktura cyfrowa, sektor technologii kosmicznych, usługi administracji publicznej.
- **Sektory Ważne:** usługi pocztowe i kurierskie, zarządzanie odpadami, produkcja chemikaliów, produkcja żywności, produkcja urządzeń medycznych, komputerów i elektroniki, maszyny i sprzęt, pojazdy i inne środki transportu, dostawcy usług cyfrowych oraz organizacje badawcze.

Podmioty te są klasyfikowane jako:

- **Podmioty Istotne:** duże organizacje, które zatrudniają ponad 250 osób lub mają roczne obroty powyżej 50 milionów euro. Obejmują one kluczowe usługi i infrastrukturę.
- **Podmioty Ważne:** mniejsze organizacje, które mimo wszystko pełnią istotną rolę w społeczeństwie i gospodarce. Kryteria obejmują liczbę pracowników i roczne obroty.

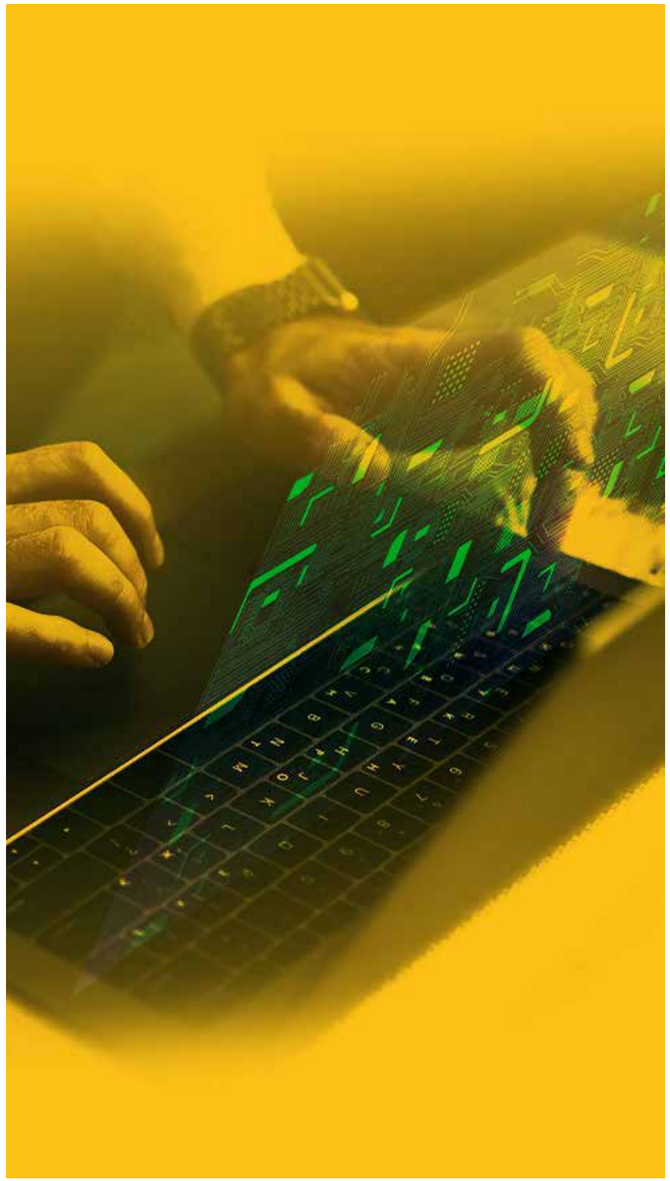


# OBOWIĄZKI PRZEDSIĘBIORSTW

Podmioty objęte dyrektywą NIS 2.0 mają obowiązek wdrożenia odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem cyberbezpieczeństwa oraz ochrony systemów informatycznych.

Kluczowe obowiązki obejmują:

- **Zarządzanie Ryzykiem:** Regularne przeprowadzanie analizy ryzyka oraz wdrożenie polityk i procedur zarządzania bezpieczeństwem systemów informatycznych.
- **Środki Techniczne:** Implementacja zabezpieczeń technicznych, takich jak firewalle, systemy wykrywania włamań, szyfrowanie danych oraz wieloczynnikowe uwierzytelnianie.
- **Szkolenia:** Przeprowadzanie regularnych szkoleń z zakresu cyberbezpieczeństwa dla pracowników, aby zwiększyć świadomość i umiejętności radzenia sobie z zagrożeniami.
- **Zgłaszanie incydentów:** Obowiązek natychmiastowego zgłaszania incydentów cyberbezpieczeństwa do odpowiednich organów krajowych, w tym CSIRT (Computer Security Incident Response Team).



# ZARZĄDZANIE INCYDENTAMI

Jednym z kluczowych elementów dyrektywy NIS 2.0 jest zarządzanie incydentami cyberbezpieczeństwa. Organizacje muszą wdrożyć procedury zgłaszania incydentów, które obejmują:

| | | |
|---|---|---|
| Wczesne Ostrzeżenie | Zgłoszenie Incydentu | Raport Końcowy |

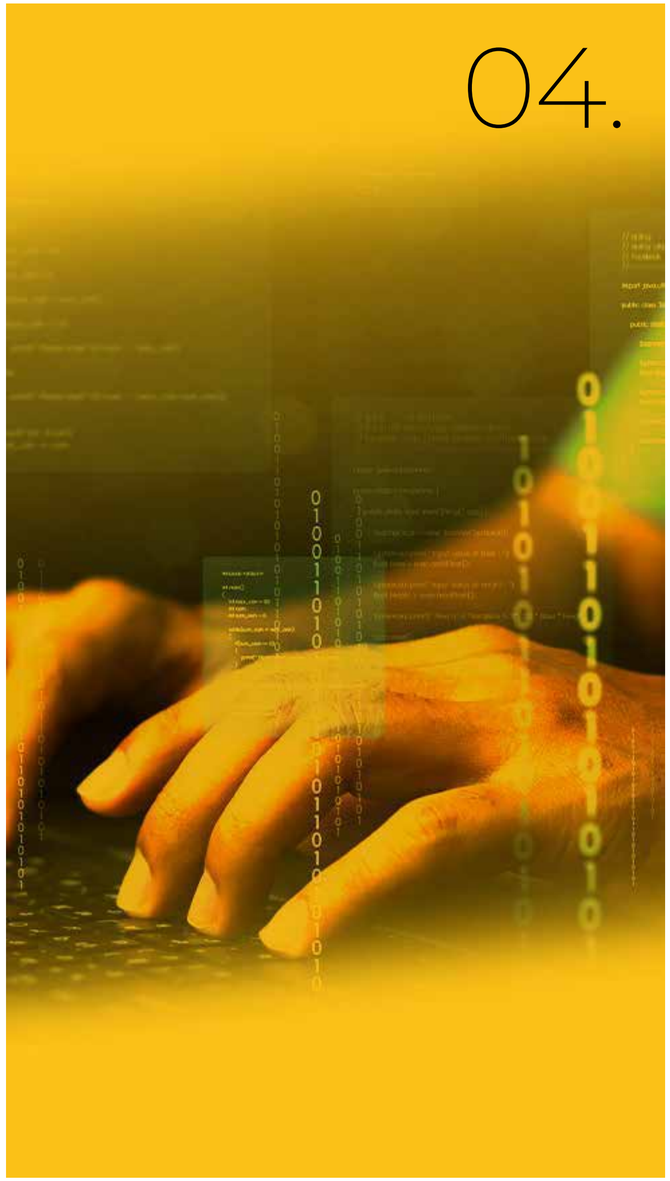
## NADZÓR I EGZEKWOWANIE

Dyrektywa NIS 2.0 wprowadza surowsze mechanizmy nadzoru i egzekwowania przepisów, mające na celu zapewnienie zgodności przedsiębiorstw z wymaganiami.

Organy krajowe będą miały uprawnienia do:

- Przeprowadzania regularnych i ad hoc audytów oraz skanów bezpieczeństwa.
- Wydawania poleceń i zaleceń dotyczących wdrożenia środków bezpieczeństwa.
- Nakładania kar finansowych za nieprzestrzeganie przepisów, które mogą sięgać do 10 milionów euro lub 2% rocznych obrotów dla podmiotów istotnych oraz 7 milionów euro lub 1,4% rocznych obrotów dla podmiotów ważnych.

04.



# ZAKRES I ZASTOSOWANIE NIS 2.0

## SEKTORY KLUCZOWE I WAŻNE

Dyrektywa NIS 2.0 znacząco rozszerza zakres sektorów objętych regulacjami, obejmując szerokie spektrum podmiotów, które są kluczowe dla funkcjonowania gospodarki i społeczeństwa.

Podmioty te zostały podzielone na dwie główne kategorie:

- Sektory Kluczowe
- Sektory Ważne

**Sektory Kluczowe** **obejmują:**

1. **Sektor Energetyczny**
   Obejmuje szeroki zakres podmiotów związanych z produkcją, dystrybucją i magazynowaniem energii, w tym energii elektrycznej, ciepłownictwa, ropy naftowej, gazu i wodoru. Wymienione są przedsiębiorstwa energetyczne, operatorzy systemów dystrybucyjnych i przesyłowych, wytwórcy, operatorzy rynku energii elektrycznej, dostawcy usług agregacji i magazynowania energii oraz operatorzy punktów ładowania.
2. **Sektor Transportowy**
   Zakres obejmuje transport lotniczy, kolejowy, wodny i drogowy. Wyróżnione podmioty to m.in. przewoźnicy lotniczy, zarządzający portami lotniczymi, operatorzy ATC, zarządcy infrastruktury kolejowej, przedsiębiorstwa kolejowe, armatorzy, operatorzy portów i systemów ruchu statków, a także organy zarządzające drogami i operatorzy ITS.
3. **Sektory Bankowość i Infrastruktura Rynków Finansowych**
   Wskazuje na instytucje kredytowe, operatorzy systemów obrotu i kontrahenci centralni jako kluczowe dla stabilności finansowej.
4. **Sektor Opieki Zdrowotnej**
   Obejmuje świadczeniodawców opieki zdrowotnej, laboratoria referencyjne UE, podmioty B+R w zakresie produktów leczniczych, producentów substancji farmaceutycznych, leków, wyrobów medycznych krytycznych w stanach zagrożenia zdrowia publicznego.
5. **Sektor Wody Pitnej i Ścieków**
   Wymienia dostawców i dystrybutorów wody pitnej oraz przedsiębiorstwa zajmujące się zbieraniem, odprowadzaniem lub oczyszczaniem ścieków.
6. **Infrastruktura Cyfrowa**
   Zawiera dostawców punktów wymiany ruchu internetowego, usług DNS, chmury, przetwarzania danych, CDN, usług zaufania, publicznych sieci i usług łączności elektronicznej.
7. **Zarządzanie Usługami ICT**
   Dotyczy dostawców usług zarządzanych i bezpieczeństwa.
8. **Administracja Publiczna**
   Wskazuje na podmioty administracyjne na szczeblu centralnym i regionalnym.
9. **Sektor technologii kosmicznych**
   Odnosi się do operatorów infrastruktury naziemnej wspierającej usługi kosmiczne.

**Sektory Ważne** **obejmują:**

1. **Sektor Usług Pocztowych i Kurierskich**
   Obejmuje operatorów świadczących usługi pocztowe i kurierskie, zapewniając krytyczną infrastrukturę dla komunikacji i dystrybucji.

2. **Sektor Gospodarowania Odpadami**
   Zawiera przedsiębiorstwa zajmujące się gospodarowaniem odpadami, kluczowe dla ochrony środowiska i zdrowia publicznego.

3. **Sektor Chemii**
   Odnosi się do przedsiębiorstw produkujących i dystrybuujących chemikalia, substancje i mieszaniny, niezbędne dla różnorodnych sektorów przemysłu.

4. **Sektor Żywności**
   Zakres obejmuje przedsiębiorstwa spożywcze zajmujące się produkcją, przetwarzaniem i dystrybucją żywności, zapewniające dostęp do podstawowych produktów żywnościowych.

5. **Sektor Produkcji**
   Obejmuje produkcję w szerokim zakresie, od wyrobów medycznych, poprzez produkcję komputerów, urządzeń elektrycznych, maszyn i urządzeń, pojazdów samochodowych, aż po pozostały sprzęt transportowy.

6. **Sektor Usług Cyfrowych**
   Zawiera dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform usług sieci społecznościowych, odgrywających kluczową rolę w cyfrowej ekonomii.

7. **Sektor Badań Naukowych**
   Odnosi się do organizacji badawczych, wspierających innowacje i rozwój technologiczny.

# KRYTERIA KLASYFIKACJI PRZEDSIĘBIORSTW

Podmioty objęte dyrektywą NIS 2.0 są klasyfikowane na podstawie ich wielkości, znaczenia oraz roli w gospodarce i społeczeństwie. Kryteria te pozwalają na określenie, czy dany podmiot jest klasyfikowany jako „istotny” czy „ważny”.

Podział ten pozwala na różnicowanie wymagań nadzoru i raportowania w zależności od znaczenia podmiotu.

| | | |
|---|---|---|
| **Podmioty Istotne** | • Duże organizacje zatrudniające ponad 250 pracowników lub generujące roczne obroty powyżej 50 milionów euro. | • Wszelkie podmioty działające w sektorach uznanych za kluczowe, niezależnie od wielkości, jeśli mają one krytyczne znaczenie dla społeczeństwa i gospodarki. |
| | • Są objęte bardziej rygorystycznymi wymaganiami nadzoru, w tym regularnymi audytami, skanami bezpieczeństwa oraz obowiązkami raportowania. | • Mogą podlegać natychmiastowym kontrolom oraz interwencjom w razie wykrycia niezgodności z przepisami. |
| **Podmioty Ważne** | • Organizacje średniej wielkości, które mimo mniejszych zasobów odgrywają istotną rolę w swojej branży lub sektorze. | • Przedsiębiorstwa spełniające kryteria ważności ze względu na swoją działalność w sektorach o dużym znaczeniu gospodarczym lub społecznym. |
| | • Podlegają mniej surowym wymaganiom nadzoru, z większym naciskiem na raportowanie ex post, czyli po zaistnieniu incydentu. | • Mogą być objęte ad hoc kontrolami w razie zgłoszenia poważnych naruszeń lub incydentów. |

05.

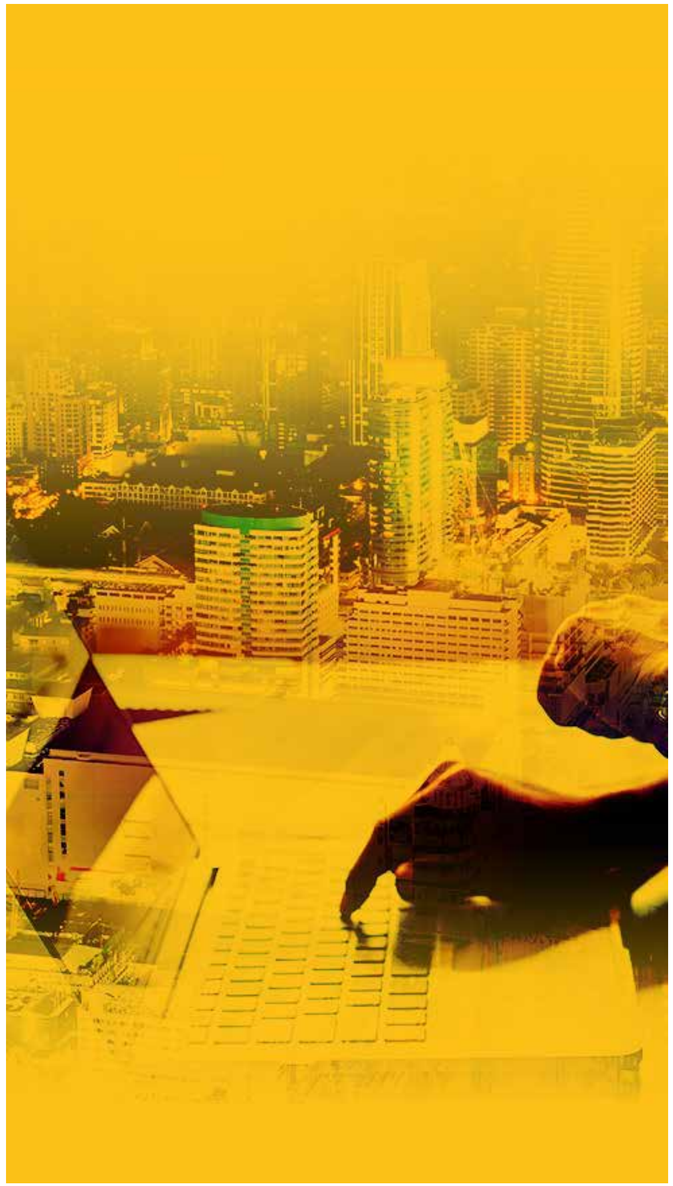
# OBOWIĄZKI PRZEDSIĘBIORSTW

## ZARZĄDZANIE RYZYKIEM CYBERBEZPIECZEŃSTWA

Jednym z kluczowych elementów Dyrektywy NIS 2.0 jest obowiązek zarządzania ryzykiem cyberbezpieczeństwa przez wszystkie podmioty objęte regulacjami. Obejmuje to identyfikację, ocenę i zarządzanie ryzykami związanymi z bezpieczeństwem sieci i systemów informatycznych. Zarządzanie ryzykiem powinno być systematyczne, kompleksowe i dostosowane do specyfiki danego przedsiębiorstwa.

**Kluczowe aspekty zarządzania ryzykiem:**

- **Analiza Ryzyka:** Regularne przeprowadzanie analiz ryzyka, które identyfikują potencjalne zagrożenia i ich wpływ na działalność przedsiębiorstwa.
- **Polityki i Procedury:** Wdrażanie i aktualizacja polityk oraz procedur zarządzania ryzykiem, które obejmują środki techniczne i organizacyjne.
- **Zarządzanie Podatnościami:** Monitorowanie i zarządzanie podatnościami w systemach informatycznych, w tym szybka reakcja na wykryte luki bezpieczeństwa.

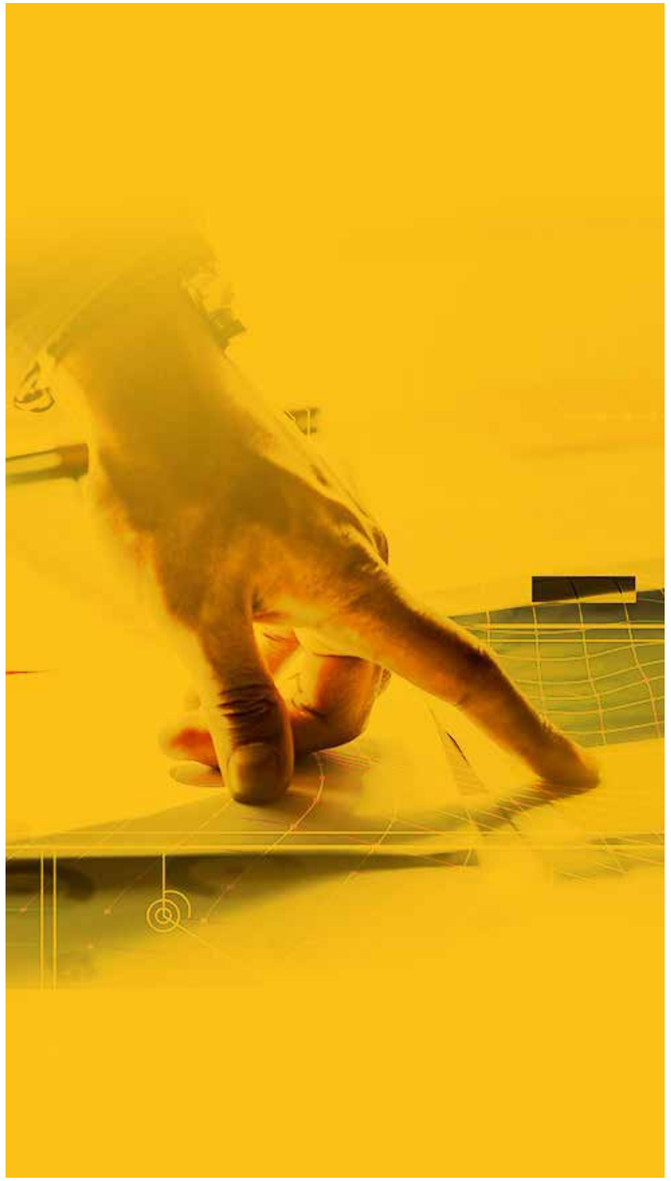


# ŚRODKI TECHNICZNE, OPERACYJNE I ORGANIZACYJNE

Dyrektywa NIS 2.0 wymaga od przedsiębiorstw wdrożenia odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych, które zapewnią ochronę przed zagrożeniami cybernetycznymi oraz minimalizują skutki incydentów.

## Wymagane środki obejmują:

- **Techniczne:** Implementacja zaawansowanych systemów zabezpieczeń, takich jak firewalle, systemy wykrywania włamań, szyfrowanie danych oraz wieloczynnikowe uwierzytelnianie.
- **Operacyjne:** utworzenie procedur reagowania na incydenty, planów ciągłości działania oraz zarządzania kryzysowego.
- **Organizacyjne:** Wyznaczenie odpowiedzialnych osób oraz zespołów ds. cyberbezpieczeństwa, prowadzenie regularnych audytów i przeglądów polityk bezpieczeństwa.

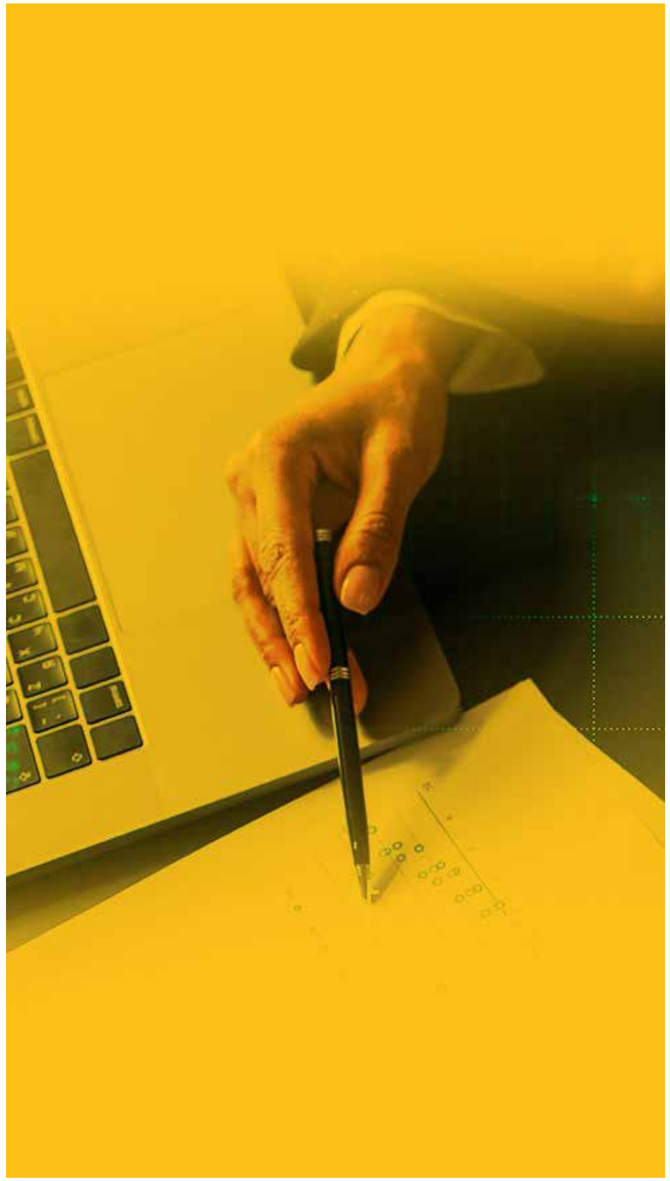


# ZGŁASZANIE INCYDENTÓW

Jednym z najważniejszych obowiązków wynikających z Dyrektywy NIS 2.0 jest obowiązek zgłaszania incydentów cyberbezpieczeństwa. Podmioty objęte dyrektywą muszą zgłaszać wszelkie incydenty, które mają istotny wpływ na świadczenie ich usług, do odpowiednich organów krajowych, takich jak CSIRT (Computer Security Incident Response Team).

**Procedura zgłaszania incydentów obejmuje:**

- **Wczesne Ostrzeżenie (w ciągu 24 godzin od wykrycia incydentu):** Informowanie odpowiednich organów o potencjalnych, poważnych incydentach, które mogą mieć wpływ na inne kraje członkowskie.
- **Zgłoszenie Incydentu (w ciągu 72 godzin od wykrycia incydentu):** Dokładne raportowanie incydentu, w tym ocena jego skali i wpływu, a także podjęte działania naprawcze.
- **Raport Końcowy:** Sporządzenie raportu końcowego lub, w przypadku trwającego incydentu, raportu z postępów i końcowego raportu po zakończeniu incydentu.

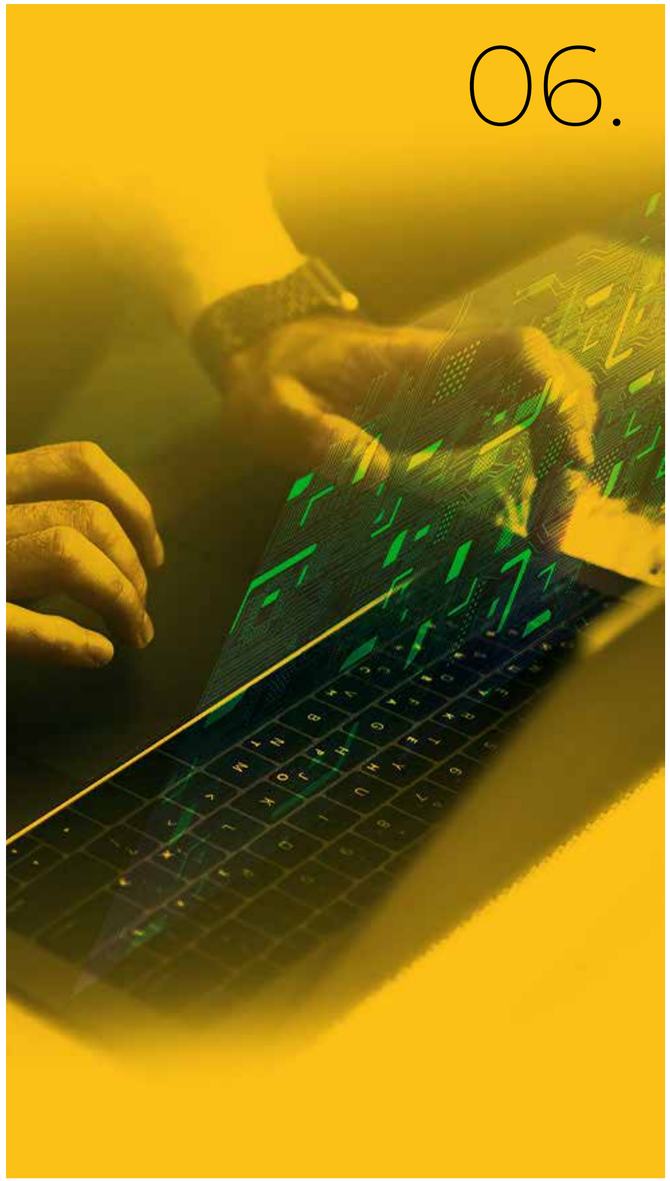


# ROLA ZARZĄDU I KADRY KIEROWNICZEJ

Dyrektywa NIS 2.0 wprowadza również wymóg zwiększenia odpowiedzialności zarządu i kadry kierowniczej za kwestie cyberbezpieczeństwa. Zarządy przedsiębiorstw są zobowiązane do nadzorowania wdrażania polityk bezpieczeństwa oraz podejmowania działań mających na celu zapewnienie zgodności z przepisami.

**Obowiązki zarządu obejmują:**

- **Nadzór nad Zarządzaniem Ryzykiem:** Regularne przeglądy i zatwierdzanie polityk zarządzania ryzykiem cyberbezpieczeństwa.
- **Szkolenia i Podnoszenie Kompetencji:** Zapewnienie odpowiednich szkoleń dla kadry kierowniczej oraz pracowników w zakresie cyberbezpieczeństwa.
- **Raportowanie i Odpowiedzialność:** Odpowiedzialność za raportowanie incydentów oraz wdrażanie działań naprawczych w przypadku wykrycia niezgodności.



06.

# ZARZĄDZANIE INCYDENTAMI

## FAZY ZGŁASZANIA INCYDENTÓW

**Wczesne Ostrzeżenie**
(w ciągu 24 godzin od wykrycia incydentu)

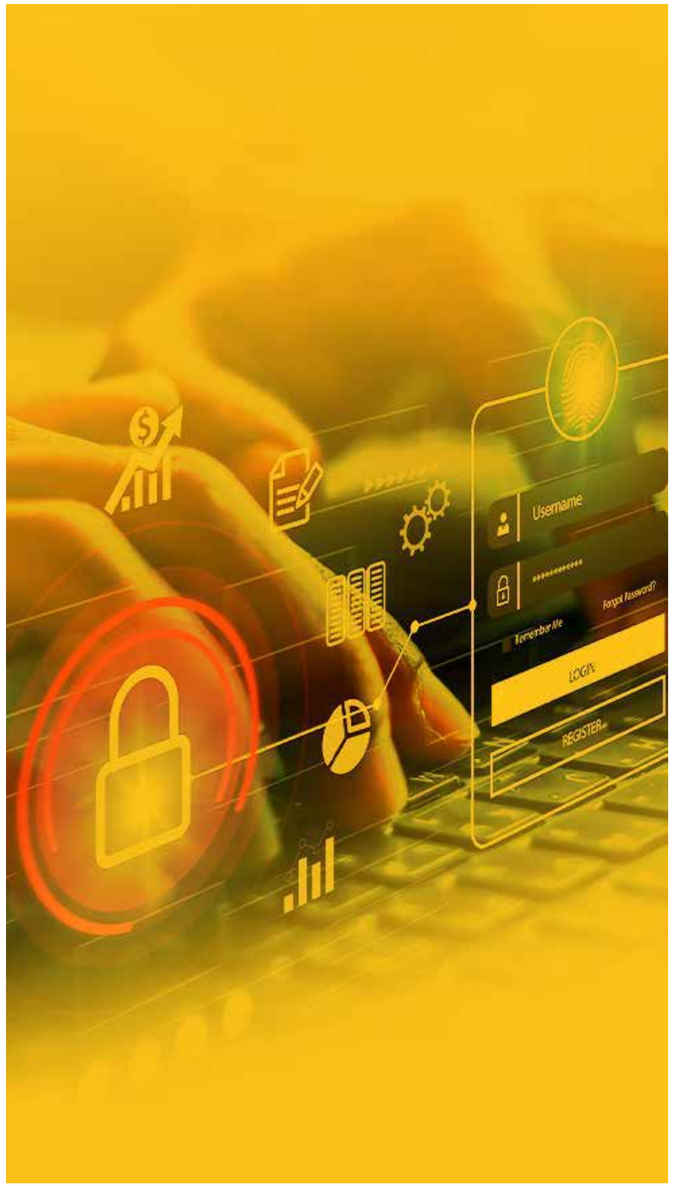
**Zgłoszenie incydentu**
(w ciągu 72 godzin od wykrycia incydentu)

**Raport Końcowy**

Podmioty objęte dyrektywą muszą bez zbędnej zwłoki zgłaszać podejrzenie incydentu, który może mieć potencjalnie poważne skutki, zwłaszcza jeśli ma wpływ na inne kraje członkowskie. Wczesne ostrzeżenie pozwala na szybkie podjęcie działań zapobiegawczych oraz koordynację międzynarodową w przypadku transgranicznych incydentów.

Incydenty cyberbezpieczeństwa muszą być zgłaszane odpowiednim organom krajowym, takim jak CSIRT (Computer Security Incident Response Team), jak najszybciej po ich wykryciu. Zgłoszenie powinno zawierać szczegółowe informacje dotyczące incydentu, takie jak jego skala, wpływ, wskaźniki kompromitacji oraz podjęte działania naprawcze.

Po zakończeniu incydentu przedsiębiorstwa są zobowiązane do sporządzenia raportu końcowego, który podsumowuje przebieg incydentu, podjęte działania oraz wnioski na przyszłość. W przypadku trwających incydentów, sporządzany jest raport z postępów, a po zakończeniu incydentu – raport końcowy.




# WYMOGI DOTYCZĄCE RAPORTOWANIA

Zgodnie z Dyrektywą NIS 2.0, każde przedsiębiorstwo musi posiadać mechanizmy zgłaszania incydentów, które umożliwiają szybką i skuteczną komunikację z odpowiednimi organami nadzoru.

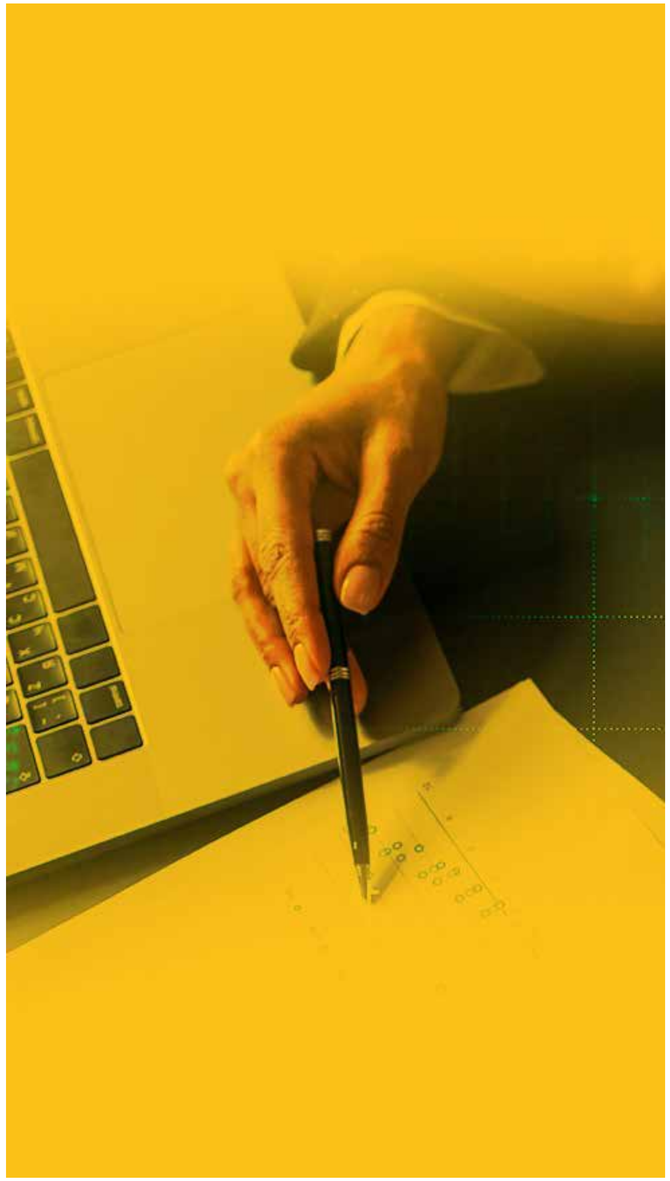
Raportowanie powinno obejmować następujące elementy:

- **Identyfikacja i Charakterystyka Incydentu:** Dokładny opis incydentu, w tym jego przyczyny, charakterystyki oraz zakresu wpływu na systemy informatyczne.
- **Ocena Skutków:** Ocena wpływu incydentu na działalność przedsiębiorstwa, w tym potencjalne skutki dla klientów oraz innych interesariuszy.
- **Działania Naprawcze:** Opis podjętych działań w celu zneutralizowania incydentu oraz przywrócenia normalnego funkcjonowania systemów.
- **Wnioski i Zalecenia:** Wnioski wyciągnięte z incydentu oraz zalecenia dotyczące zapobiegania podobnym incydentom w przyszłości.

# ROLA CSIRT I INNYCH ORGANÓW

CSIRT oraz inne odpowiednie organy krajowe odgrywają kluczową rolę w zarządzaniu incydentami cyberbezpieczeństwa. Ich zadania obejmują:

- **Koordynacja Działań:** Współpraca z przedsiębiorstwami oraz innymi organami w celu skoordynowania działań mających na celu neutralizację incydentu oraz minimalizację jego skutków.
- **Wsparcie Techniczne:** Dostarczanie wsparcia technicznego oraz doradztwa w zakresie zarządzania incydentami i wprowadzania środków naprawczych.
- **Monitorowanie i Raportowanie:** Monitorowanie zgłaszanych incydentów oraz tworzenie raportów z ich przebiegu, które są następnie analizowane w celu wyciągnięcia wniosków na przyszłość.



# PRAKTYCZNE WSKAZÓWKI DLA PRZEDSIĘBIORSTW

Aby skutecznie zarządzać incydentami cyberbezpieczeństwa, przedsiębiorstwa powinny wdrożyć następujące działania:

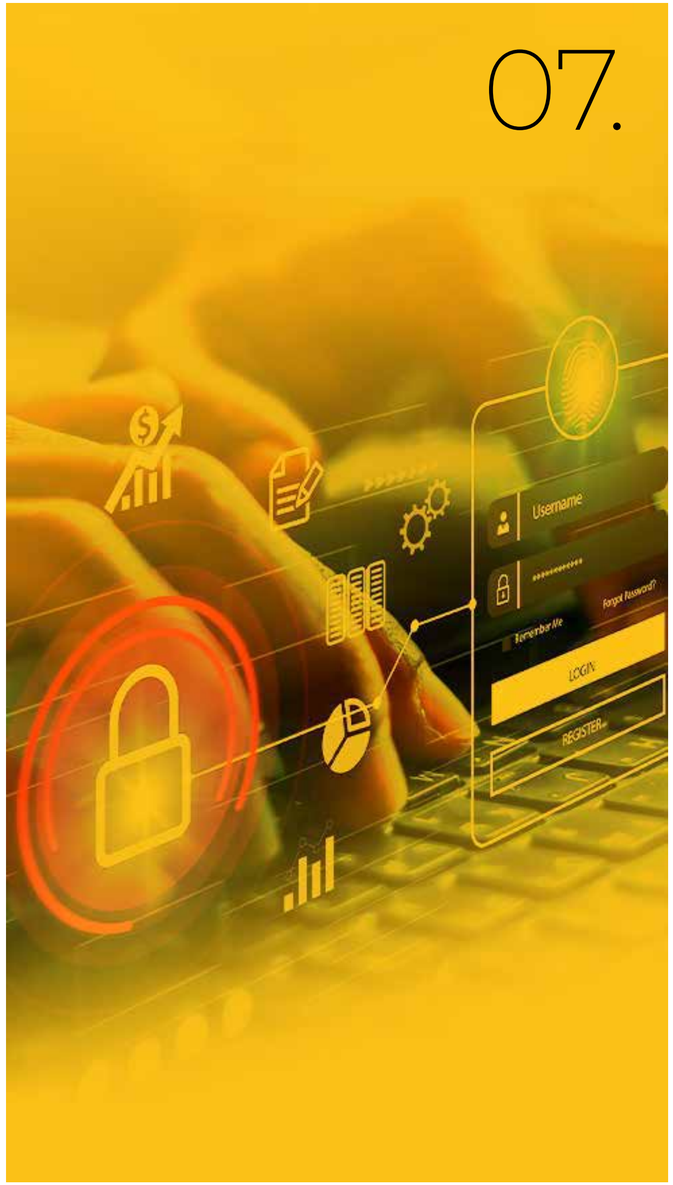
1. **Utworzenie Planu Zarządzania Incydentami**
   Opracowanie szczegółowego planu zarządzania incydentami, który zawiera procedury zgłaszania, analizowania i reagowania na incydenty.

2. **Regularne Szkolenia**
   Przeprowadzanie regularnych szkoleń dla pracowników z zakresu rozpoznawania i zgłaszania incydentów cyberbezpieczeństwa.

3. **Testowanie i Aktualizacja**
   Regularne testowanie i aktualizacja procedur zarządzania incydentami, aby zapewnić ich skuteczność w przypadku rzeczywistych zagrożeń.

4. **Współpraca z CSIRT**
   Utrzymywanie stałej współpracy z CSIRT oraz innymi odpowiednimi organami, aby zapewnić szybki przepływ informacji oraz wsparcie w przypadku incydentów.

07.




# NADZÓR I EGZEKWOWANIE

## UPRAWNIENIA ORGANÓW NADZORU

Dyrektywa NIS 2.0 wprowadza bardziej rygorystyczne mechanizmy nadzoru i egzekwowania przepisów dotyczących cyberbezpieczeństwa. Organy nadzoru w poszczególnych państwach członkowskich UE mają szerokie uprawnienia do monitorowania zgodności przedsiębiorstw z wymaganiami dyrektywy.

**Kluczowe uprawnienia obejmują:**

- **Regularne Audyty:** Organy nadzoru mogą przeprowadzać regularne audyty systemów bezpieczeństwa, aby sprawdzić zgodność z wymaganiami NIS 2.0. Audyty te mogą być zarówno planowane, jak i ad hoc, w zależności od potrzeb.
- **Skanowanie Bezpieczeństwa:** W ramach nadzoru mogą być przeprowadzane skany bezpieczeństwa, mające na celu wykrycie potencjalnych luk w zabezpieczeniach.
- **Kontrole Dokumentacji:** Organy nadzoru mogą żądać dostarczenia dokumentacji potwierdzającej wdrożenie odpowiednich środków bezpieczeństwa oraz zarządzania ryzykiem.

# KARY I SANKCJE ZA NIEPRZESTRZEGANIE PRZEPISÓW

NIS 2.0 wprowadza surowe sankcje za nieprzestrzeganie przepisów dotyczących cyberbezpieczeństwa. Kary te mają na celu zapewnienie, że przedsiębiorstwa traktują kwestie bezpieczeństwa poważnie i podejmują niezbędne działania w celu ochrony swoich systemów informatycznych.

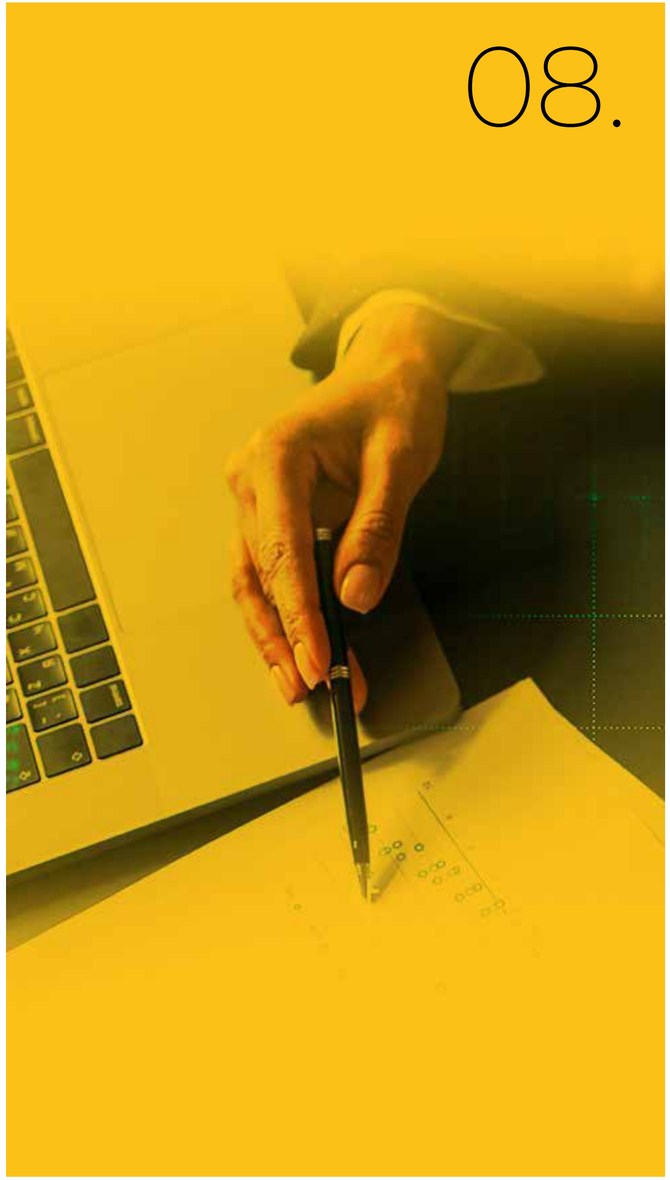
**Rodzaje kar obejmują:**

- **Kary Finansowe:** Organy nadzoru mogą nakładać wysokie kary finansowe na przedsiębiorstwa, które nie spełniają wymagań NIS 2.0. Dla podmiotów istotnych kary mogą sięgać do **10 milionów euro** lub **2% rocznych obrotów**, a dla podmiotów ważnych – do **7 milionów euro** lub **1,4% rocznych obrotów.**
- **Nakazy i Polecenia:** Organy nadzoru mogą wydawać nakazy usunięcia niezgodności, w tym polecenia wdrożenia określonych środków bezpieczeństwa w określonym terminie.
- **Zawieszenia działalności:** W przypadku poważnych naruszeń, organy nadzoru mogą zawiesić zezwolenie na prowadzenie działalności przez przedsiębiorstwo.

# OCHRONA DANYCH OSOBOWYCH

W przypadku wykrycia przez właściwe organy, że naruszenia przez podmioty kluczowe lub ważne mogą prowadzić do naruszenia ochrony danych osobowych, te organy niezwłocznie informują o tym organy nadzorcze ds. ochrony danych osobowych.

08.



# ODPOWIEDZIALNOŚĆ KIEROWNICTWA

## WYMAGANIA WOBEC ZARZĄDU I KADRY KIEROWNICZEJ

Dyrektywa NIS 2.0 znacząco zwiększa odpowiedzialność zarządu oraz kadry kierowniczej za zapewnienie zgodności z przepisami dotyczącymi cyberbezpieczeństwa. Zarządy muszą aktywnie uczestniczyć w zarządzaniu ryzykiem oraz wdrażaniu odpowiednich środków zabezpieczających, co ma na celu zwiększenie ogólnego poziomu ochrony w organizacjach.

**Kluczowe wymagania obejmują:**

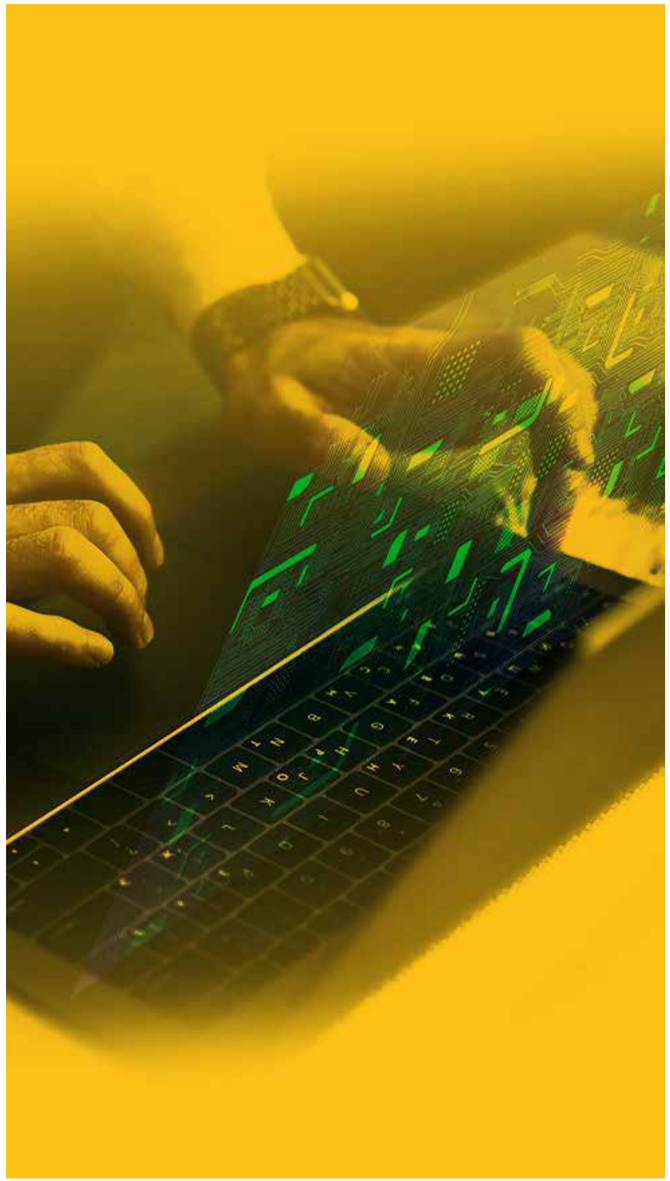
- **Zatwierdzanie Polityk i Procedur:** Zarząd musi regularnie przeglądać i zatwierdzać polityki oraz procedury zarządzania ryzykiem cyberbezpieczeństwa, aby zapewnić ich aktualność i skuteczność.
- **Nadzór nad Wdrażaniem Środków Bezpieczeństwa:** Kadra kierownicza jest odpowiedzialna za nadzorowanie wdrażania środków technicznych, operacyjnych i organizacyjnych, które mają na celu ochronę systemów informatycznych przed zagrożeniami.

# SZKOLENIA I PODNOSZENIE KOMPETENCJI

W ramach NIS 2.0, zarząd oraz kadra kierownicza muszą posiadać odpowiednie kompetencje i wiedzę w zakresie cyberbezpieczeństwa. Regularne szkolenia są kluczowe dla zapewnienia, że osoby odpowiedzialne za zarządzanie mają świadomość aktualnych zagrożeń oraz najlepszych praktyk w dziedzinie bezpieczeństwa informatycznego.

**Obowiązki w zakresie szkoleń obejmują:**

- **Szkolenia dla Zarządu:** Członkowie zarządu muszą uczestniczyć w szkoleniach, które pozwolą im zrozumieć zagrożenia cybernetyczne oraz sposoby zarządzania ryzykiem.
- **Szkolenia dla Pracowników:** Organizacje muszą zapewnić regularne szkolenia z zakresu cyberbezpieczeństwa dla wszystkich pracowników, aby zwiększyć ogólną świadomość i zdolność do reagowania na incydenty.

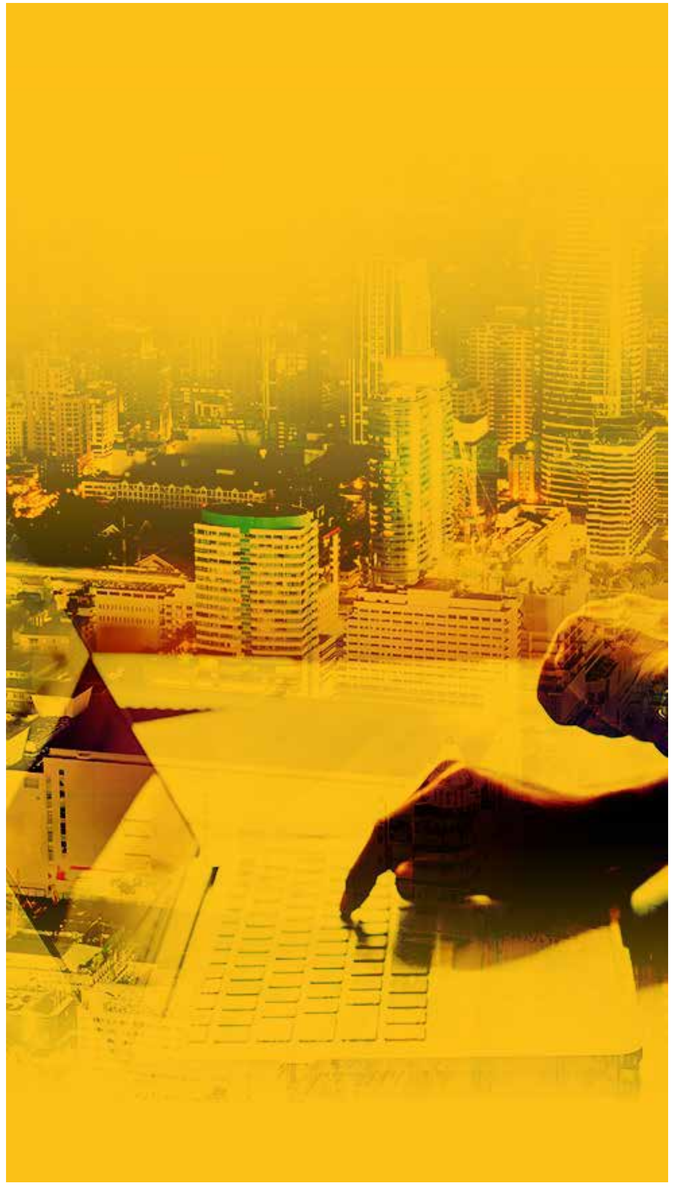


# KONSEKWENCJE BRAKU ZGODNOŚCI Z PRZEPISAMI

NIS 2.0 wprowadza surowe konsekwencje dla zarządu i kadry kierowniczej w przypadku nieprzestrzegania przepisów dotyczących cyberbezpieczeństwa. Obejmuje to zarówno odpowiedzialność finansową, jak i prawną, co ma na celu zapewnienie, że kwestie bezpieczeństwa są traktowane priorytetowo na najwyższym szczeblu zarządzania.

## Możliwe konsekwencje obejmują:

- **Kary Finansowe:** Nakładanie kar finansowych osoby odpowiedzialne za brak zgodności z przepisami.
- **Odpowiedzialność Karna:** Osoby zarządzające mogą ponosić odpowiedzialność karną za zaniedbania w zakresie zarządzania cyberbezpieczeństwem.

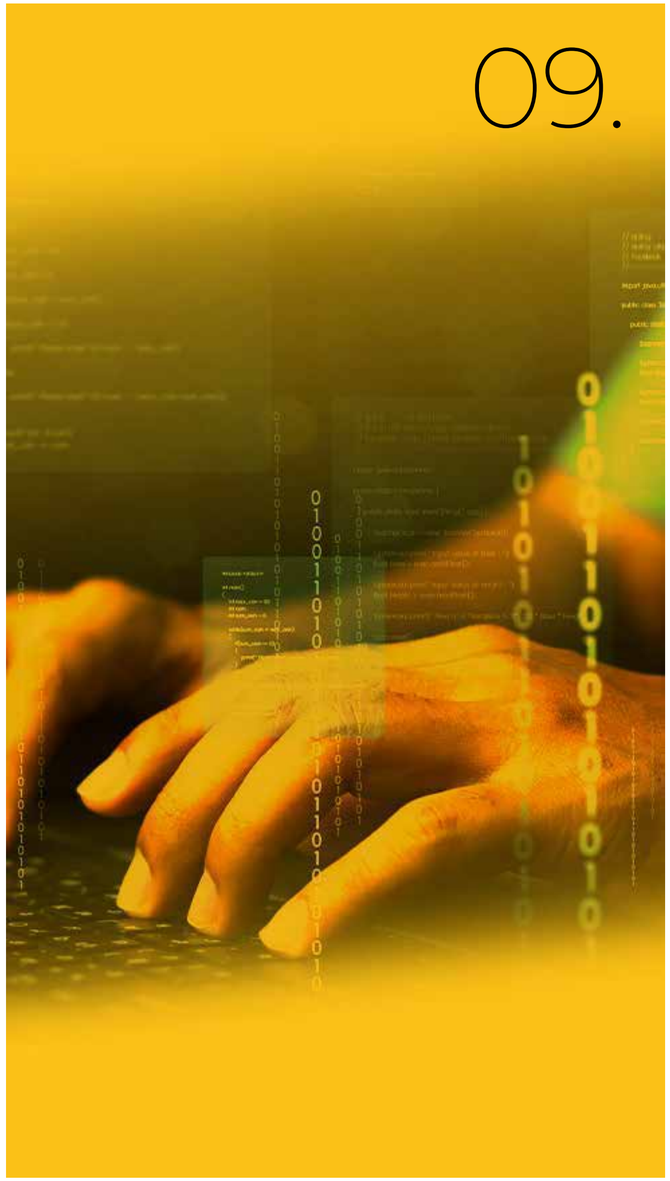


# PRAKTYCZNE WSKAZÓWKI DLA ZARZĄDU

Aby skutecznie zarządzać ryzykiem cyberbezpieczeństwa i zapewnić zgodność z NIS 2.0, zarząd powinien wdrożyć następujące działania:

1. **Utworzenie Dedykowanego Zespołu**
   Powierzenie zarządzania cyberbezpieczeństwem dedykowanemu zespołowi specjalistów, który będzie odpowiedzialny za monitorowanie, analizowanie i reagowanie na zagrożenia.
2. **Regularne Przeglądy i Audyty**
   Przeprowadzanie regularnych przeglądów i audytów systemów bezpieczeństwa w celu identyfikacji i eliminacji potencjalnych słabości.
3. **Komunikacja i Współpraca**
   Zapewnienie skutecznej komunikacji i współpracy między różnymi działami organizacji oraz zewnętrznymi partnerami, aby wspólnie przeciwdziałać zagrożeniom cybernetycznym.
4. **Inwestycje w Technologie Bezpieczeństwa**
   Inwestowanie w najnowsze technologie i rozwiązania zabezpieczające, które mogą skutecznie chronić systemy informatyczne przed atakami.
5. **Zewnętrznie niezależne oceny**
   Wykorzystywanie zewnętrznych, niezależnych ekspertów do okresowej weryfikacji skuteczności systemów bezpieczeństwa, jak i technicznej odporności systemów informatycznych.

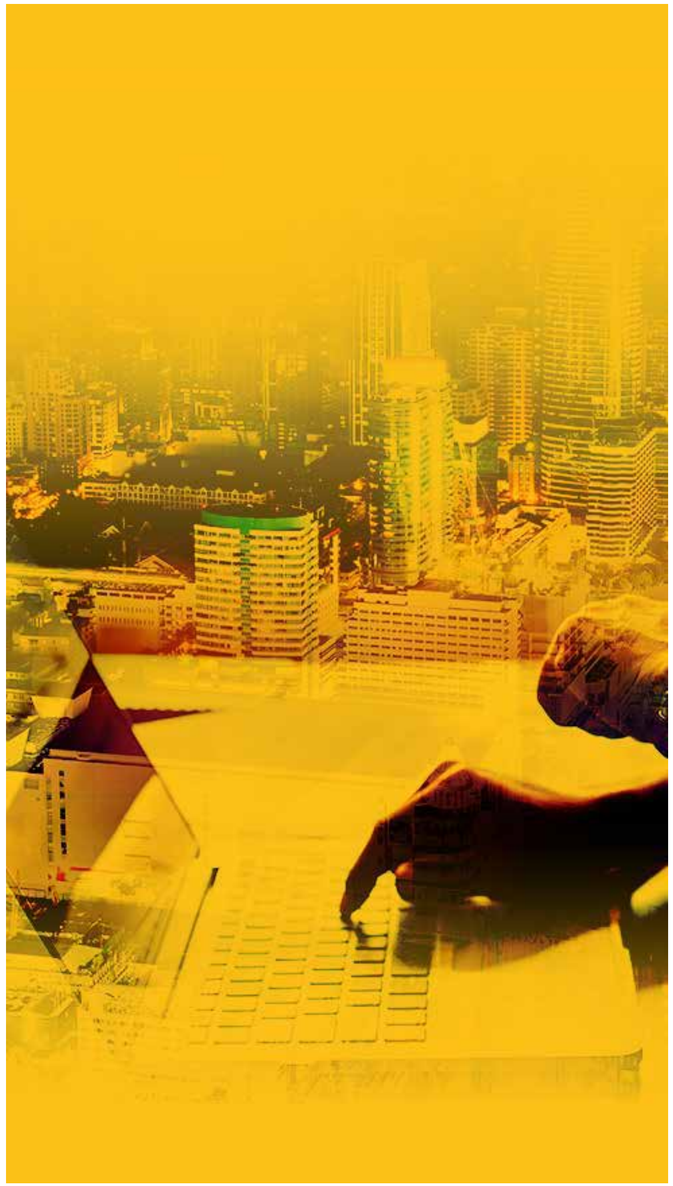
09.



# USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

## CEL I ZAKRES USTAWY

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) została wprowadzona w celu zwiększenia poziomu cyberbezpieczeństwa w Polsce poprzez wdrożenie odpowiednich środków zabezpieczających i zarządzających ryzykiem. Ustawa ta jest kluczowym elementem harmonizacji polskich przepisów z Dyrektywą NIS 2.0, mając na celu szczegółowe określenie wymogów cyberbezpieczeństwa.

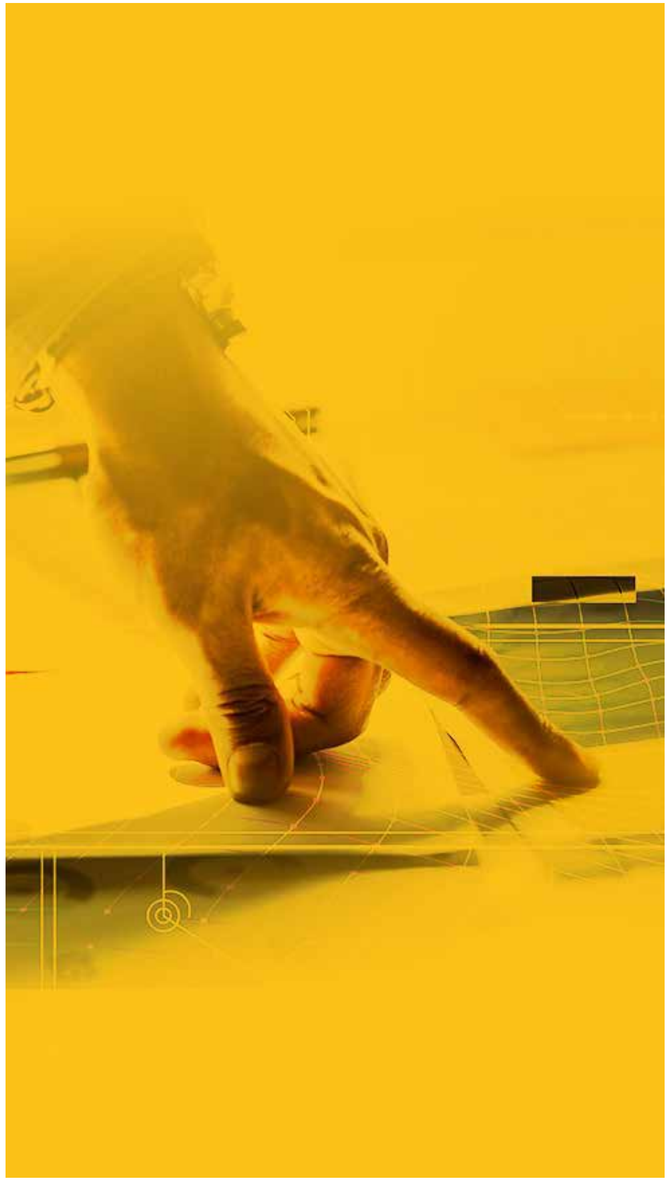


# HARMONIZACJA Z DYREKTYWĄ NIS 2.0

Ustawa o KSC jest bezpośrednio powiązana z Dyrektywą NIS 2.0, której celem jest ujednolicenie przepisów dotyczących cyberbezpieczeństwa w całej Unii Europejskiej. Dzięki temu możliwe jest zapewnienie spójności i skuteczności działań na poziomie krajowym i europejskim.

## Główne elementy harmonizacji obejmują:

- **Zakres Podmiotów:** Ustawa obejmuje szeroki zakres podmiotów, w tym sektor publiczny, prywatny oraz dostawców usług cyfrowych, zgodnie z definicjami zawartymi w Dyrektywie NIS 2.0.
- **Zarządzanie Ryzykiem:** Wprowadzenie obowiązku przeprowadzania regularnych analiz ryzyka oraz wdrażania odpowiednich środków technicznych i organizacyjnych.
- **Zgłaszanie Incydentów:** Obowiązek zgłaszania incydentów cyberbezpieczeństwa do krajowych organów nadzoru.



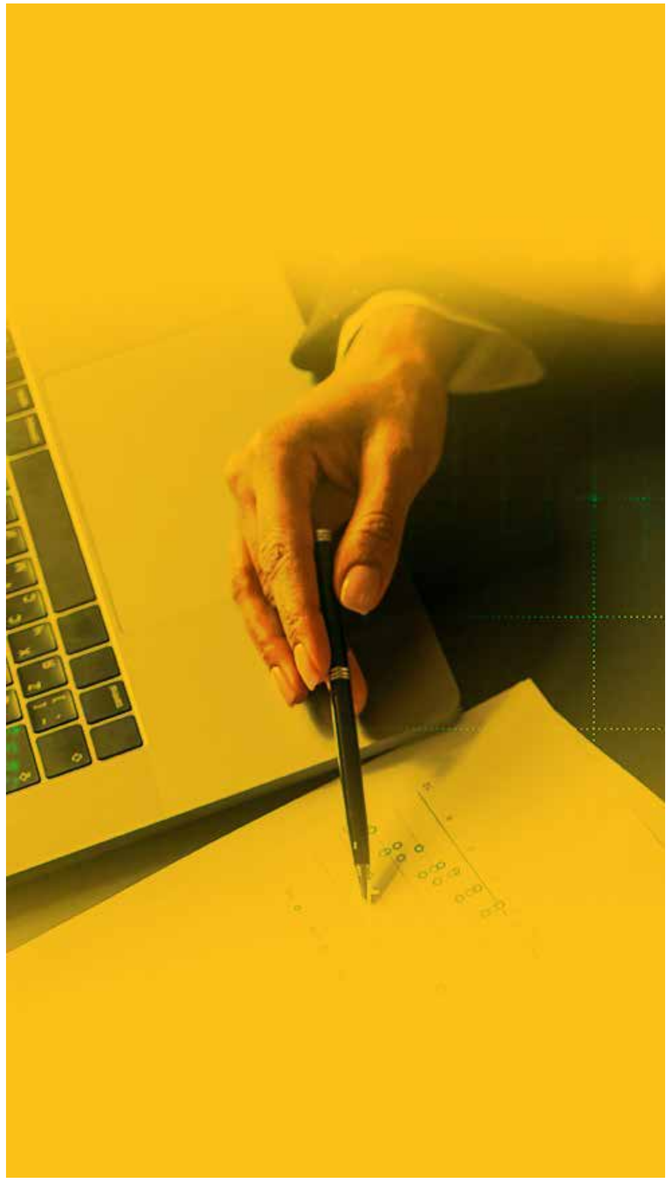
# GŁÓWNE ZAŁOŻENIA I DEFINICJE

Ustawa o KSC zawiera kluczowe definicje i założenia, które określają ramy prawne zarządzania cyberbezpieczeństwem w Polsce.

**Incydent Cyberbezpieczeństwa** – Zdarzenie, które ma negatywny wpływ na bezpieczeństwo sieci i systemów informatycznych.

**Podmioty KSC** – Organizacje, które są zobowiązane do przestrzegania przepisów ustawy, w tym podmioty sektora publicznego i prywatnego oraz dostawcy usług cyfrowych.

**CSIRT** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, odpowiedzialny za koordynację działań związanych z zarządzaniem incydentami.

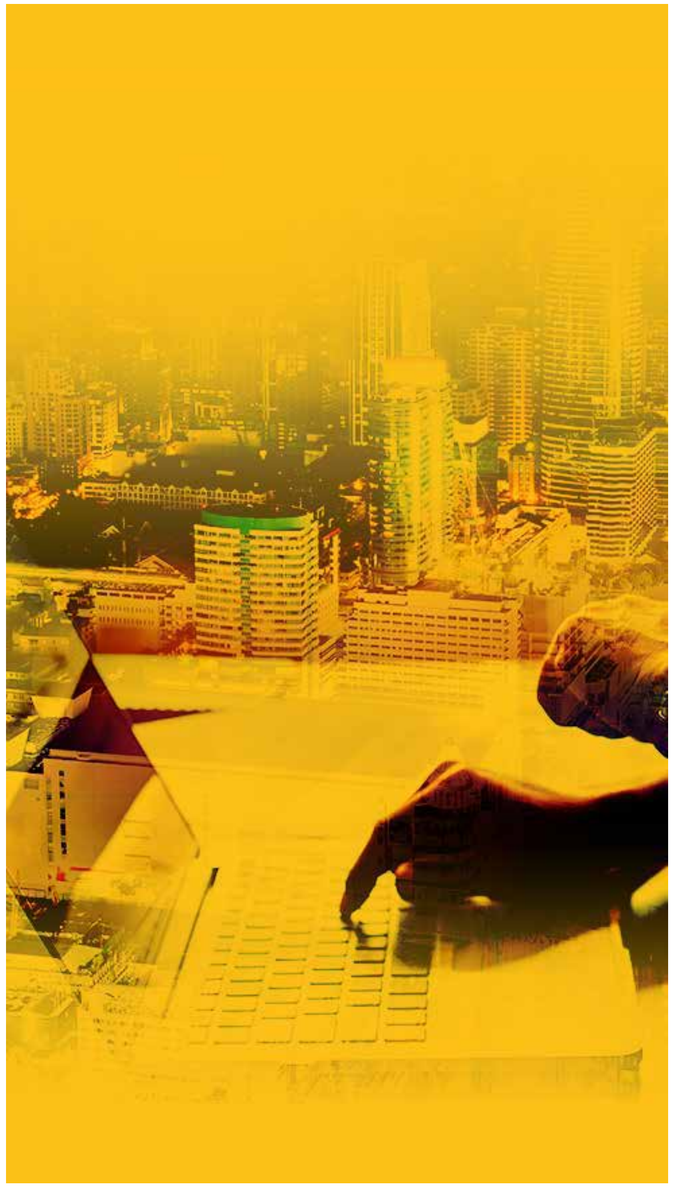


# OBOWIĄZKI PRZEDSIĘBIORSTW WG USTAWY O KSC

Podmioty objęte ustawą o KSC mają szereg obowiązków związanych z zapewnieniem bezpieczeństwa swoich systemów informatycznych.

**Główne obowiązki obejmują:**

- **Środki Zabezpieczające:** Wdrożenie odpowiednich środków technicznych, operacyjnych i organizacyjnych w celu ochrony przed zagrożeniami cybernetycznymi.
- **Zgłaszanie Incydentów:** Obowiązek natychmiastowego zgłaszania incydentów cyberbezpieczeństwa do CSIRT lub innych właściwych organów.
- **Współpraca z Organami Krajowymi:** Utrzymywanie stałej współpracy z krajowymi organami nadzoru oraz uczestnictwo w działaniach koordynacyjnych i szkoleniach.

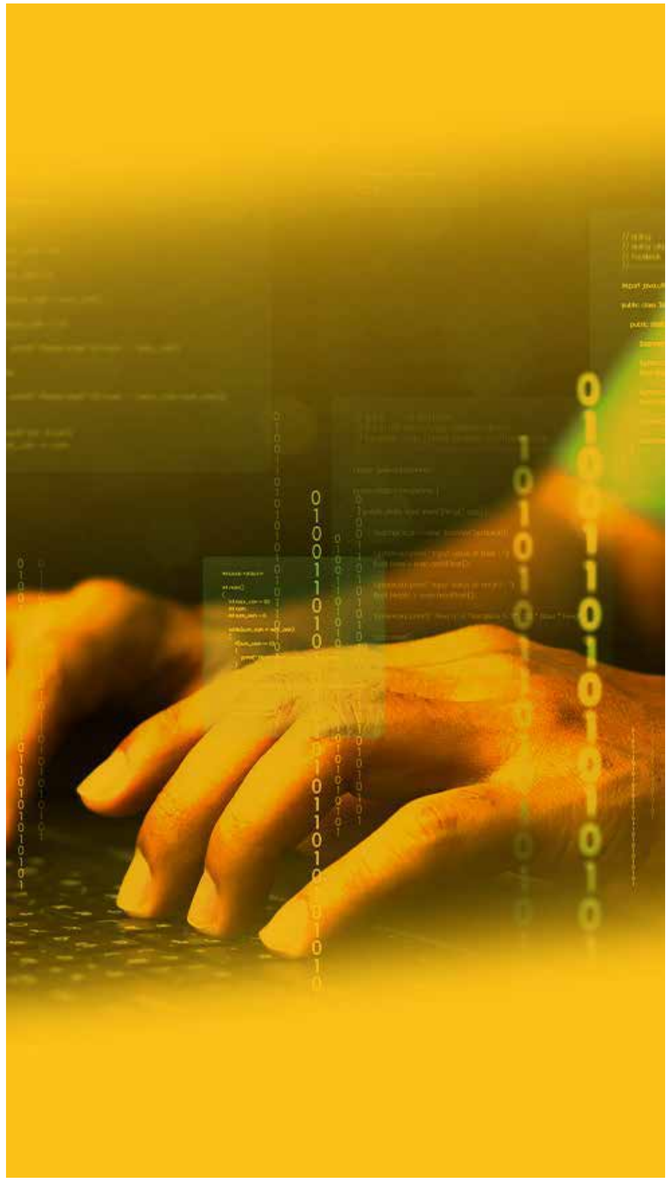


# WYMAGANIA DOTYCZĄCE STANDARDÓW ISO

Ustawa o KSC nakłada na przedsiębiorstwa obowiązek oparcia się na europejskich standardach cyberbezpieczeństwa, takimi jak m.in. normy ISO. Standardy te stanowią podstawę do budowy skutecznych systemów zarządzania bezpieczeństwem informacji (SZBI).

**Dobre praktyki obejmują budowanie systemów w oparciu o:**

- **ISO/IEC 27001:** Standard ten określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji. Organizacje muszą wdrożyć polityki i procedury zgodne z ISO/IEC 27001, aby skutecznie zarządzać ryzykiem związanym z bezpieczeństwem informacji.
- **ISO/IEC 22301:** Standard dotyczący zarządzania ciągłością działania, który pomaga organizacjom przygotować się na zakłócenia działalności, takie jak incydenty cyberbezpieczeństwa. Wdrożenie ISO/IEC 22301 pomaga w zapewnieniu ciągłości działania i szybkim przywróceniu normalnego funkcjonowania po incydencie.



# IMPLEMENTACJA I PRAKTYCZNE WSKAZÓWKI

Implementacja przepisów ustawy o KSC wymaga od przedsiębiorstw wdrożenia szeregu działań mających na celu zwiększenie poziomu cyberbezpieczeństwa.

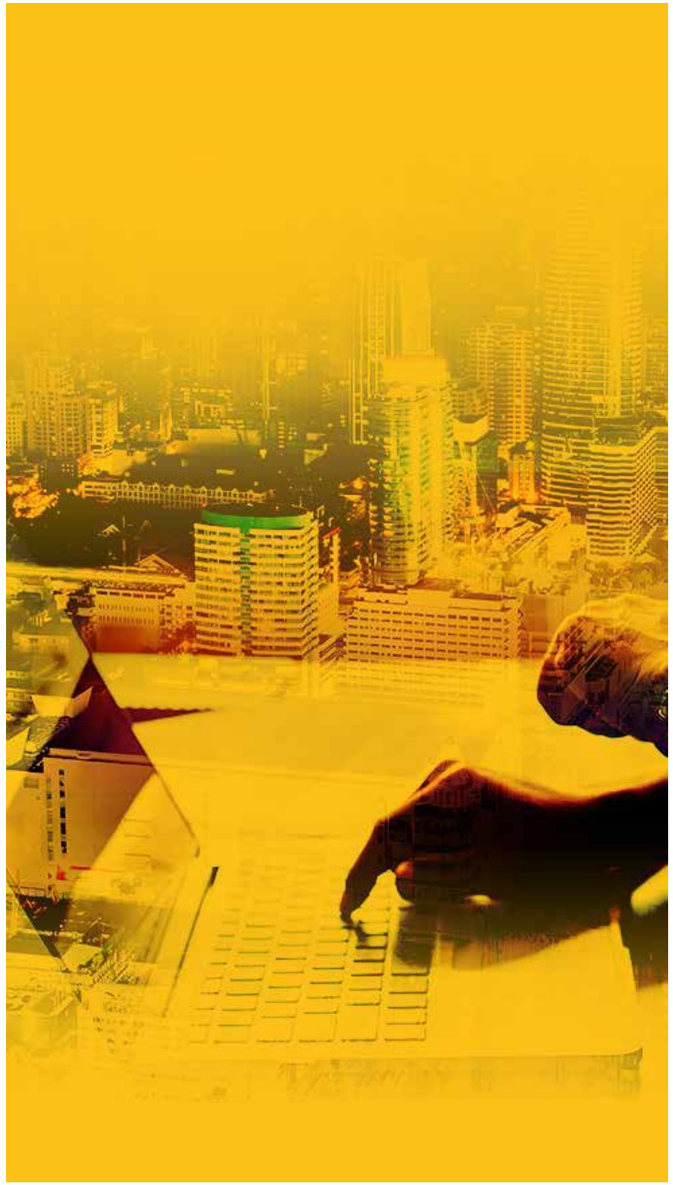
**Kluczowe kroki obejmują:**

- **Audyt Cyberbezpieczeństwa:** Przeprowadzenie kompleksowego audytu w celu identyfikacji potencjalnych zagrożeń i słabości systemów informatycznych.
- **Plan Zarządzania Ryzykiem:** Opracowanie i wdrożenie planu zarządzania ryzykiem, który obejmuje środki prewencyjne oraz procedury reagowania na incydenty.
- **Polityki i Procedury:** Wdrożenie Polityk i procedur
- **Szkolenia dla Pracowników:** Zapewnienie regularnych szkoleń dla pracowników w zakresie rozpoznawania zagrożeń i reagowania na incydenty cyberbezpieczeństwa.
- **Wdrożenie Technicznych i Organizacyjnych Środków Bezpieczeństwa:** Implementacja technicznych i organizacyjnych środków bezpieczeństwa ograniczających ryzyko do akceptowalnego poziomu.

# 10. OBOWIĄZKI PRZEDSIĘBIORSTW WG USTAWY O KSC

| Obszar/termin | Podmiot kluczowy | Podmiot ważny |
|---|---|---|
| **Wdrożenie obowiązków (podmioty objęte zakresem w dniu wejścia w życie)** | | |
| **Do 6 miesięcy od wejścia w życie** | Opracowanie i udokumentowanie analizy ryzyka; wdrożenie systemu zarządzania bezpieczeństwem informacji oraz rozwiązań z zakresu ciągłości działania adekwatnych do ryzyka; ustanowienie procesu i procedur zarządzania incydentami; wdrożenie adekwatnych środków technicznych i organizacyjnych (w tym w obszarze zależności i łańcucha dostaw). | Jak dla podmiotu kluczowego (pakiet wdrożeniowy). |
| **Do 24 miesięcy od wejścia w życie** | Przeprowadzenie **pierwszego niezależnego audytu** cyberbezpieczeństwa. | Co do zasady brak automatyzmu – audyt może wynikać z działań nadzorczych (np. żądanie organu / treść decyzji). |
| **Wdrożenie obowiązków (podmioty objęte zakresem po wejściu w życie – decyzja/tryb objęcia)** | | |
| **Do 6 lub 12 miesięcy (zgodnie z decyzją/ trybem objęcia)** | Realizacja pakietu wdrożeniowego: analiza ryzyka, SZBI/ciągłość działania, proces zarządzania incydentami, środki techniczne i organizacyjne adekwatne do ryzyka (w tym zależności). | Jak dla podmiotu kluczowego. |
| **Do 24 miesięcy od doręczenia decyzji** | Przeprowadzenie **pierwszego niezależnego audytu** cyberbezpieczeństwa. | Analogicznie – audyt zasadniczo jako instrument nadzorczy (w zależności od wymogów organu). |

| Obszar/termin | Podmiot kluczowy | Podmiot ważny |
|---|---|---|
| **Audyty cykliczne oraz przekazywanie raportów** | | |
| **Nie rzadziej niż raz na 3 lata** | Zapewnienie cyklicznego **niezależnego audytu** cyberbezpieczeństwa. | Co do zasady brak obowiązku cyklicznego audytu w standardowym reżimie; możliwe na podstawie decyzji/wezwania organu. |
| **Do 3 dni roboczych od otrzymania raportu** | Przekazanie raportu z audytu do organu właściwego. | Jeżeli audyt został przeprowadzony na podstawie wymogu – przekazanie raportu analogicznie. |
| **Zgłaszanie incydentów (SLA raportowe)** | | |
| **Do 24 godzin od wykrycia** | Przekazanie wczesnego ostrzeżenia / zgłoszenie podejrzenia incydentu do właściwego CSIRT / organu. | Jak dla podmiotu kluczowego. |
| **Do 72 godzin od wykrycia** | Zgłoszenie incydentu zawierające co najmniej: skalę i wpływ, wskaźniki kompromitacji, podjęte i planowane działania korygujące/naprawcze. | Jak dla podmiotu kluczowego. |
| **Raport postępu (jeżeli incydent trwa / na żądanie)** | Przekazywanie raportów pośrednich (w trakcie/na żądanie) w toku obsługi incydentu. | Jak dla podmiotu kluczowego. |
| **Raport końcowy – co do zasady do 1 miesiąca** (lub raport postępu + final po zakończeniu) | Sporządzenie i przekazanie raportu końcowego podsumowującego przebieg incydentu, skutki oraz wnioski/korekty kontrolne. | Jak dla podmiotu kluczowego. |



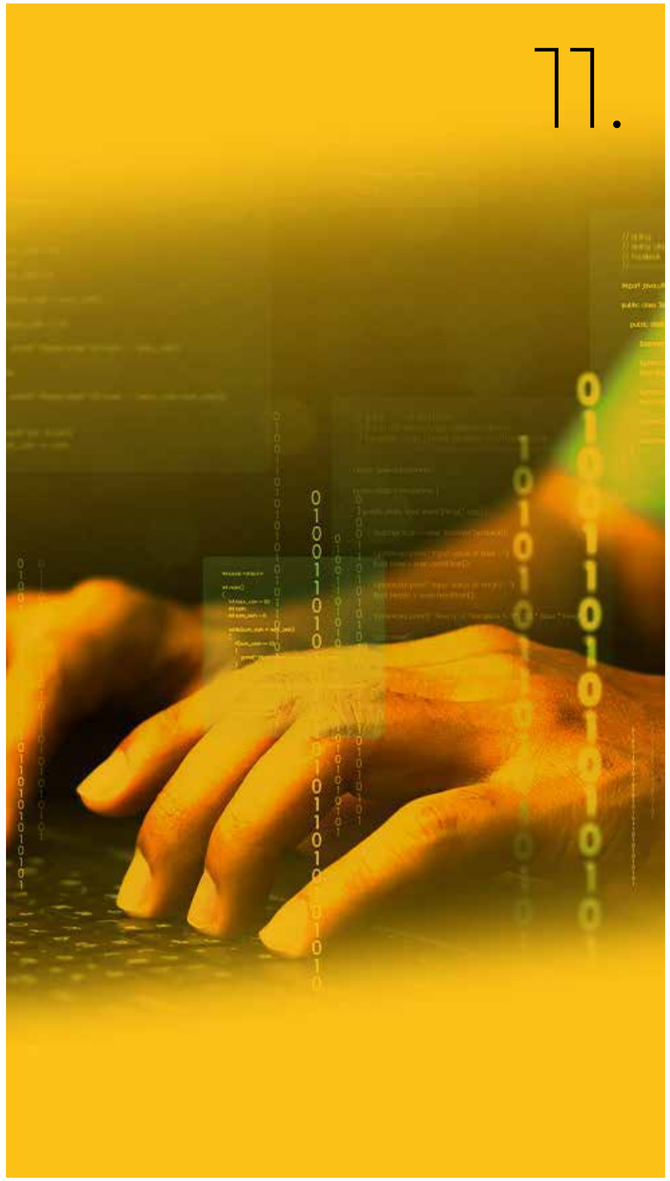
# ŚRODKI ZABEZPIECZAJĄCE

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) nakłada na przedsiębiorstwa obowiązek wdrożenia odpowiednich środków zabezpieczających, które mają na celu ochronę przed zagrożeniami cybernetycznymi oraz minimalizację skutków incydentów.

**Kluczowe środki obejmują:**

- **Techniczne Środki Bezpieczeństwa:** Implementacja zaawansowanych technologii zabezpieczających, takich jak firewalle, systemy wykrywania włamań (IDS/IPS), szyfrowanie danych, systemy zarządzania dostępem oraz wieloczynnikowe uwierzytelnianie (MFA).
- **Operacyjne Środki Bezpieczeństwa:** Utworzenie procedur reagowania na incydenty, planów ciągłości działania oraz zarządzania kryzysowego. Przedsiębiorstwa muszą także przeprowadzać regularne testy penetracyjne oraz oceny bezpieczeństwa swoich systemów informatycznych.
- **Organizacyjne Środki Bezpieczeństwa:** Wyznaczenie odpowiedzialnych osób oraz zespołów ds. cyberbezpieczeństwa, prowadzenie regularnych audytów i przeglądów polityk i procedur bezpieczeństwa oraz wdrażanie polityk zarządzania ryzykiem.

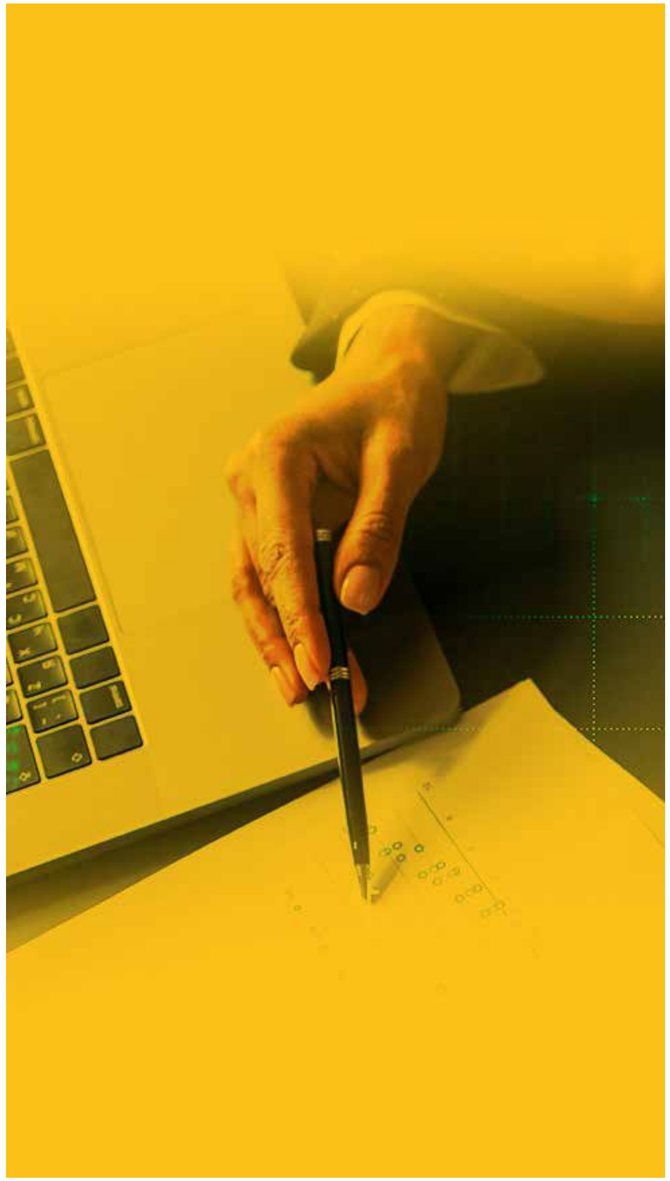
11.



# IMPLEMENTACJA USTAWY O KSC DLA RÓŻNYCH TYPÓW ORGANIZACJI

## ORGANIZACJE PODLEGAJĄCE NIS1 I POPRZEDNIM WYMAGANIOM UKSC

Dla organizacji, które już wcześniej podlegały przepisom NIS1 oraz wcześniejszym wymaganiom Ustawy o Krajowym Systemie Cyberbezpieczeństwa, wdrożenie NIS 2.0 i aktualizacji UKSC wiąże się z rozszerzeniem i uaktualnieniem istniejących mechanizmów zabezpieczeń oraz procedur.



# WDROŻENIE NOWYCH WYMAGAŃ NIS 2.0 I UKSC

**Analiza luki**

Przeprowadzenie analizy luki i określenie niezbędnych zmian.

**Plan dostosowania**

Przygotowanie planu dostosowania organizacji do nowych wymagań, w tym określenie niezbędnych zadań, terminów i zasobów.

**Wdrożenie wymagań**

Zgodnie z planem dostosowania wdrażanie poszczególnych rozwiązań organizacyjnych i technicznych.

# ORGANIZACJE DOTYCHCZAS NIEPODLEGAJĄCE NIS1 I POPRZEDNIM WYMAGANIOM KSC

Dla organizacji, które dotychczas nie podlegały przepisom NIS ani wcześniejszym wymaganiom Ustawy o Krajowym Systemie Cyberbezpieczeństwa, wdrożenie nowych regulacji wiąże się z koniecznością stworzenia od podstaw odpowiednich mechanizmów zabezpieczeń i procedur.

## ETAP 1 AUDYT 0 – ANALIZA LUKI

**Cel:** Ocena bieżącego stanu organizacji w kontekście wymagań NIS 2.0 i UKSC, identyfikacja luk w zabezpieczeniach i procedurach.

**Działania:**

- **Przegląd Bieżących Praktyk:** Zidentyfikowanie i dokumentowanie obecnych praktyk zarządzania bezpieczeństwem informacyjnym.
- **Ocena Wymagań:** Porównanie obecnych praktyk z wymaganiami NIS 2.0 i UKSC, aby zidentyfikować luki.
- **Raport z Analizy Luki:** Sporządzenie raportu wskazującego obszary wymagające poprawy oraz rekomendacje dotyczące działań naprawczych.

**Czas trwania:** Około 6–8 tygodni.

## ETAP 2 ANALIZA RYZYKA I ZARZĄDZANIE

**Cel:** Przeprowadzenie analizy ryzyka oraz wdrażanie polityk zarządzania ryzykiem cyberbezpieczeństwa.

**Działania:**

- **Polityki Zarządzania Ryzykiem:** Opracowanie i wdrożenie polityk zarządzania ryzykiem.
- **Ocena Zagrożeń:** Identyfikacja potencjalnych zagrożeń i ocena ich wpływu.
- **Przygotowanie planu ograniczenia ryzyka:** Przygotowanie planu wdrożenia rozwiązań organizacyjnych i technicznych ograniczających ryzyko.

**Czas trwania:** Około 2–4 tygodnie.

## ETAP 3 ZARZĄDZANIE INCYDENTAMI

**Cel:** Utworzenie procesu i procedur zarządzania incydentami cyberbezpieczeństwa.

**Działania:**

- **Procedury Zgłaszania:** Opracowanie procesów i procedur zarządzania incydentami bezpieczeństwa oraz ich zgłaszania do odpowiednich organów, takich jak CSIRT.
- **Współpraca z Organami:** Nawiązanie współpracy z krajowymi i międzynarodowymi organami odpowiedzialnymi za cyberbezpieczeństwo.
- **Testowanie Procedur:** Przetestowanie procedur zarządzania incydentami poprzez symulacje i ćwiczenia.

**Czas trwania:** Około 2–4 tygodnie.

## ETAP 4 ŚRODKI TECHNICZNE I PROCEDURALNE

**Cel:** Implementacja podstawowych technologii zabezpieczających i dokumentacji bezpieczeństwa: polityki i procedury.

**Działania:**

- **Polityki i Procedury Bezpieczeństwa:** Opracowanie polityk procedur dotyczących bezpieczeństwa informacji, w tym zarządzania dostępem, zarządzania podatnościami i patchingiem, monitorowania, zarządzania łańcuchem dostaw, zarządzania oprogramowaniem, przeglądów i audytów.
- **Zabezpieczenia Techniczne:** Instalacja firewalli, systemów wykrywania włamań, systemów monitorowania i korelacji zdarzeń, szyfrowanie danych i wprowadzenie wieloczynnikowego uwierzytelniania.

**Czas trwania:** W zależności od zidentyfikowanych ryzyk.

## ETAP 5 SZKOLENIA I PODNOSZENIE KOMPETENCJI

**Cel:** Zapewnienie regularnych szkoleń z zakresu cyberbezpieczeństwa dla pracowników oraz kadry zarządzającej.

**Działania:**

- **Programy Szkoleniowe:** Organizowanie cyklicznych szkoleń i warsztatów z zakresu najnowszych praktyk i zagrożeń w cyberbezpieczeństwie.
- **Podnoszenie Świadomości:** Wdrożenie programów podnoszenia świadomości pracowników na temat cyberzagrożeń i najlepszych praktyk bezpieczeństwa.

**Czas trwania:** Na bieżąco

## ETAP 6 AUDYT I PRZEGLĄDY

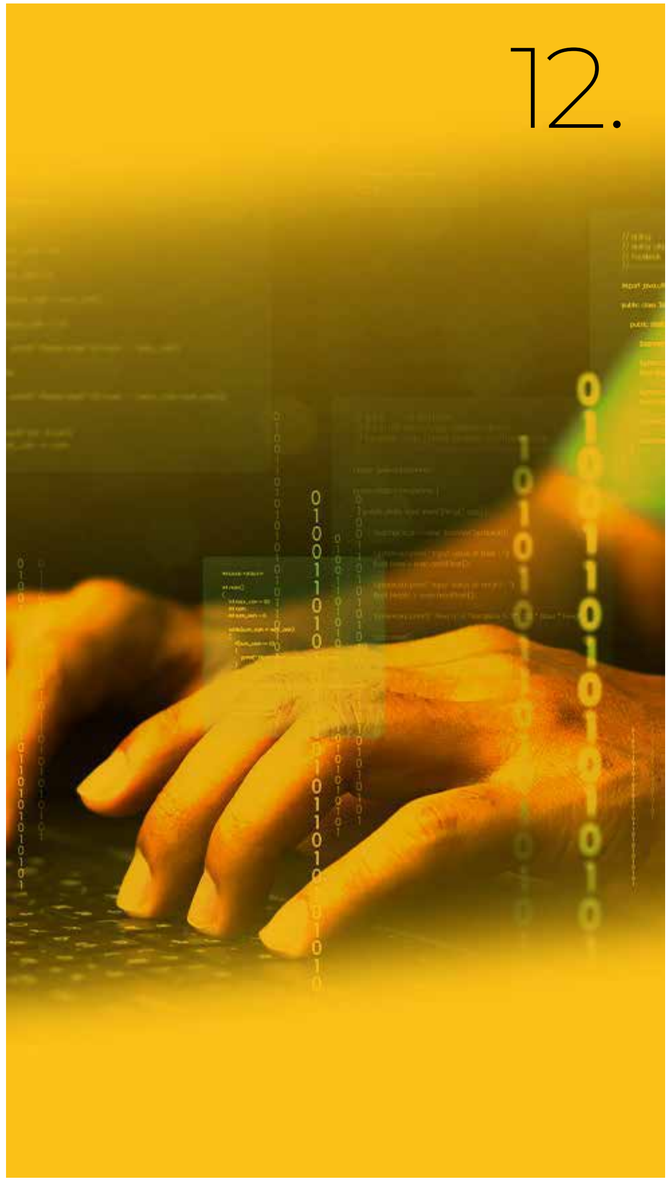
**Cel:** Testowanie skuteczności wdrożonych rozwiązań poprzez regularne audyty, przeglądy, inspekcje, testy.

**Działania:**

- **Wewnętrzne Procesy Audytu:** Ustanowienie wewnętrznych procesów weryfikacji skuteczności systemów bezpieczeństwa, w tym prowadzenia audytu, które będą sprawdzać zgodność z przepisami NIS 2.0 i UKSC.
- **Dokumentacja i Dowody:** Przygotowanie dokumentacji i dowodów na wdrożenie odpowiednich środków zabezpieczających.
- **Regularne Przeglądy:** Przeprowadzanie regularnych przeglądów wewnętrznych w celu identyfikacji i naprawy potencjalnych słabości.

**Czas trwania:** Na bieżąco

12.



# WYBÓR ODPOWIEDNIEJ FIRMY AUDYTORSKIEJ LUB DORADCZEJ

## KLUCZOWE KWALIFIKACJE I CERTYFIKATY

Wybór odpowiedniej firmy audytorskiej lub doradczej do zapewnienia zgodności z przepisami NIS 2.0 oraz Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UKSC) jest kluczowy dla spełnienia wszystkich wymogów regulacyjnych i bezpieczeństwa. Poniżej przedstawiono kluczowe kwalifikacje i certyfikaty, które powinny posiadać firmy specjalizujące się w audycie i doradztwie w zakresie NIS 2.0 oraz UKSC.

# WYMAGANE UMIEJĘTNOŚCI I KOMPETENCJE

Aby zapewnić, że firma audytorska lub doradcza posiada niezbędną wiedzę i doświadczenie, należy zwrócić uwagę na następujące umiejętności i kompetencje:

1. **Umiejętności Analizy i Oceny Kontroli**
   - **Analiza Techniczna i Ewaluacja Kontroli:** Kluczowe dla oceny procesów, systemów oraz skuteczności kontroli technicznych.
   - **Zastosowanie Profesjonalnego Osądu:** Krytyczne dla oceny skomplikowanych scenariuszy i podejmowania świadomych decyzji dotyczących zgodności.
2. **Znajomość Profesjonalnych Standardów i Regulacji**
   - **Wiedza Prawna i Regulacyjna:** Głębokie zrozumienie przepisów dotyczących cyberbezpieczeństwa, takich jak NIS 2.0, UKSC, RODO oraz specyficznych wytycznych sektorowych.
   - **Polityki Kontroli Jakości Firmy:** Wdrożone procedury kontroli jakości zapewniające wysokie standardy w audytach i ocenach zgodności.
   - **Wiedza Sektorowa:** Znajomość specyficznych dla branży wyzwań związanych z zgodnością, np. w sektorze zdrowia, finansach, telekomunikacji, data center oraz przemysłowych systemów informatycznych (OT/ICS/SCADA).

1. **Specyficzne Umiejętności w Różnych Zakresach Zgodności**
   - **Zarządzanie Ryzykiem Cyberbezpieczeństwa:** Doświadczenie w ustanawianiu ram zarządzania ryzykiem, przeprowadzaniu ocen ryzyka oraz wdrażaniu strategii ograniczania ryzyka.
   - **Ochrona Prywatności i Bezpieczeństwo Danych:** Dogłębna wiedza na temat przepisów dotyczących ochrony danych osobowych i zasad bezpieczeństwa.
   - **Znajomość Specyficznych Technologii:** Głębokie zrozumienie technologii stosowanych w różnych branżach, takich jak OT/ICS/SCADA, systemy telekomunikacyjne, data center, urządzenia medyczne, oraz bezpieczne tworzenie kodu, chmury i wykorzystanie AI.

# REKOMENDOWANE CERTYFIKATY

Certyfikaty członków zespołu powinny odzwierciedlać ich doświadczenie w zakresie cyberbezpieczeństwa, zgodności oraz audytu.

1. **Certyfikaty Specyficzne dla Cyberbezpieczeństwa:**
   - **CISM (Certified Information Security Manager):** Zarządzanie bezpieczeństwem informacji.
   - **CISSP (Certified Information Systems Security Professional):** Zaawansowana wiedza z zakresu bezpieczeństwa.
   - **CEH (Certified Ethical Hacker):** Techniczne testowanie bezpieczeństwa.
2. **Certyfikaty Specyficzne dla Prywatności i Bezpieczeństwa:**
   - **CDPSE (Certified Data Privacy Solutions Engineer):** Rozwiązania z zakresu prywatności danych.
   - **CCAK (Certificate of Cloud Auditing Knowledge):** Audyt bezpieczeństwa chmury.
   - **GICSP (Global Industrial Cyber Security Professional):** Specjalizacja w zakresie bezpieczeństwa systemów OT/ICS.
   - **CSSLP (Certified Secure Software Lifecycle Professional):** Bezpieczne tworzenie oprogramowania.
   - **CCSP (Certified Cloud Security Professional):** Bezpieczeństwo chmury.
1. **Certyfikaty Specyficzne dla Zarządzania Ryzykiem i Audytu:**
   - **CISA (Certified Information Systems Auditor):** Wiedza ekspercka w audycie systemów informatycznych.
   - **CRISC (Certified in Risk and Information Systems Control):** Zarządzanie ryzykiem i kontrolą systemów informatycznych.
   - **ISO/IEC 27001 Lead Auditor:** Zarządzanie bezpieczeństwem informacji.
   - **ISO/IEC 22301 Lead Auditor:** Zarządzanie ciągłością działania.

# IMPLEMENTACJA STANDARDÓW

Firmy audytorskie i doradcze powinny mieć praktyczną wiedzę na temat różnych standardów dotyczących cyberbezpieczeństwa oraz specyficznych technologii:

1. **Standardy bezpieczeństwa i ciągłości działania:**
   - **ISO/IEC 27001:** Zarządzanie bezpieczeństwem informacji.
   - **ISO/IEC 22301:** Zarządzanie ciągłością działania.
2. **Standardy dla Systemów OT/ICS:**
   - **NIST SP 800-82:** Wytyczne bezpieczeństwa dla systemów automatyki przemysłowej i sterowania.
   - **ISA/IEC 62443:** Standardy bezpieczeństwa dla systemów automatyki przemysłowej i sterowania.

1. **Standardy dla Bezpiecznego Tworzenia Kodów:**
   - **OWASP (Open Web Application Security Project):** Standardy bezpieczeństwa aplikacji webowych.
   - **Software Assurance Maturity Model (SAMM):** Model zapewnienia dojrzałości bezpieczeństwa oprogramowania.
2. **Standardy dla Bezpieczeństwa Chmury:**
   - **CSA (Cloud Security Alliance) Security Guidance:** Wytyczne bezpieczeństwa dla technologii chmury.
   - **NIST SP 500-291:** Wytyczne bezpieczeństwa chmury.
3. **Standardy dla Analizy Technicznej i Cyberbezpieczeństwa:**
   - **MITRE ATT&CK:** Standard do opisu i klasyfikacji cyberzagrożeń.
   - **CWE (Common Weakness Enumeration):** Katalog typowych słabości bezpieczeństwa.

# PROCES WYBORU FIRMY AUDYTORSKIEJ LUB DORADCZEJ

Wybór odpowiedniej firmy audytorskiej lub doradczej to złożony proces, który wymaga oceny nie tylko kwalifikacji i certyfikatów, ale także zrozumienia specyficznych wyzwań i ryzyk związanych z branżą oraz zgodnością z NIS 2.0 i UKSC.

Kluczowe kroki obejmują:

### Ocena Kwalifikacji

- Sprawdzenie czy firma posiada odpowiednie certyfikaty i doświadczenie w obszarze cyberbezpieczeństwa i zgodności.
- Ocena umiejętności analizy technicznej i znajomości regulacji.

### Zrozumienie Sektorowe

- Upewnienie się, że firma ma doświadczenie w danym sektorze i rozumie unikalne wyzwania związane z zgodnością.

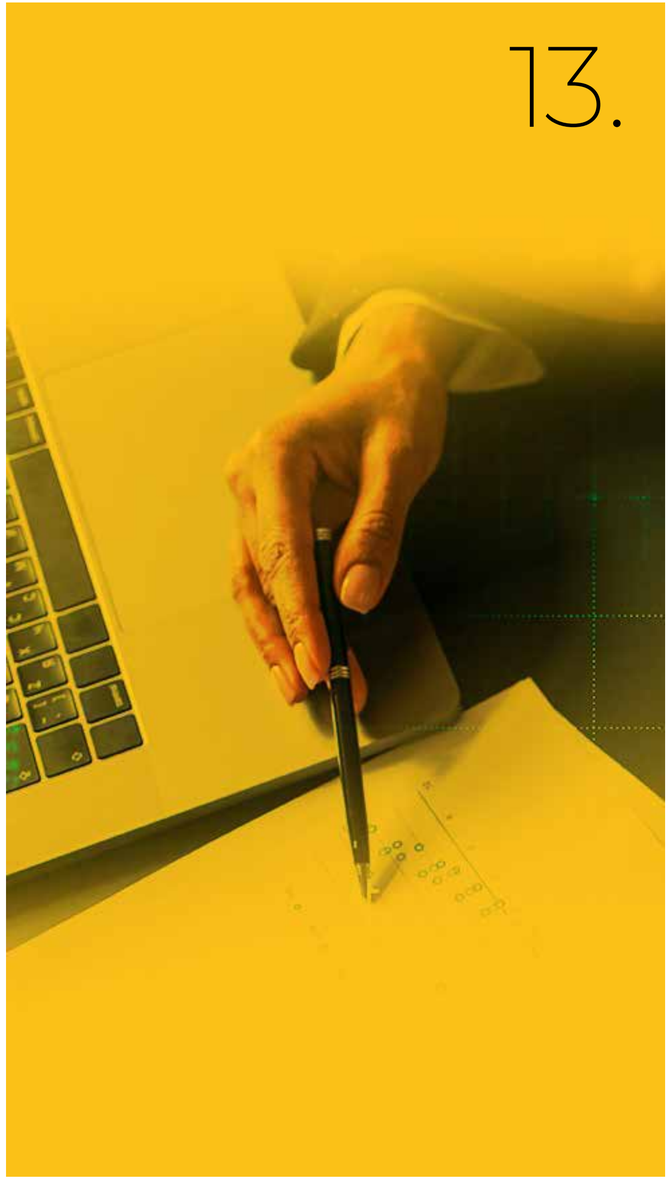
### Sprawdzenie Referencji

- Zasięgnięcie opinii innych klientów firmy oraz analiza studiów przypadków.

### Kompleksowość Usług

- Upewnienie się, że firma oferuje pełen zakres usług, od analizy ryzyka, poprzez audyty, po wsparcie w implementacji środków zabezpieczających.

13.



# NASZE PODEJŚCIE DO USŁUG ZGODNOŚCI Z NIS 2.0 I UKSC

W BW Advisory sp. z o.o. rozumiemy, że każda organizacja jest unikalna, a podejście bez analizy kontekstu biznesowego nie działa w kontekście usług zgodności z NIS 2.0 i Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UKSC). Naszym celem jest dostarczanie spersonalizowanych usług, które odpowiadają specyficznemu profilowi ryzyka, technologii i wymogom regulacyjnym każdej organizacji.

# ZROZUMIENIE TWOJEGO UNIKALNEGO ŚRODOWISKA BIZNESOWEGO

1. **Ocena Natury i Złożoności**
   - **Struktura Biznesowa i Ryzyka Branżowe:** Oceniamy strukturę biznesową, specyficzne ryzyka branżowe oraz złożoność operacji technologicznych i zarządzania. Dotyczy to zrozumienia unikalnych wyzwań i ryzyk związanych z różnymi sektorami, takimi jak opieka zdrowotna, finanse, telekomunikacja, centra danych oraz przemysłowe systemy kontrolne (OT/ICS/SCADA).
   - **Struktury Cyberbezpieczeństwa i Kontroli:** Szczególną uwagę zwracamy na branże podatne na cyberataki oraz organizacje z zdecentralizowanymi lub złożonymi strukturami kontroli wewnętrznej, tak aby zapewnić kompleksową ochronę przed potencjalnymi zagrożeniami.
2. **Uwzględnienie Wielkości i Modelu Biznesowego**
   - **Analiza Modelu Biznesowego:** Analizujemy złożoność modelu biznesowego, biorąc pod uwagę różnorodność usług technologicznych, złożoność systemów oraz ryzyko reputacji. To pomaga nam zrozumieć specyficzne potrzeby i wyzwania, przed którymi stają organizacje.
   - **Ocena Zasobów:** Dla większych organizacji uwzględniamy ich zasoby, aby uprościć proces angażowania, zapewniając, że nasze rozwiązania są zarówno kompleksowe, jak i praktyczne.

1. **Świadczone Usługi**
   - **Zakres i Złożoność Usług:** Przeprowadzamy szczegółową ocenę zakresu i złożoności świadczonych usług technologicznych, od prostych narzędzi automatyzacji po złożone systemy zarządzania danymi i kontrolami przemysłowymi (ICS/OT).
   - **Analiza Danych:** Zwracamy uwagę na charakter przetwarzanych danych, aby skutecznie dostosować nasze usługi.
2. **Natura i Wielkość Systemu Technologicznego**
   - **Ocena Komponentów Systemu:** Analizujemy komponenty systemu istotne dla świadczonych usług technologicznych, w tym architekturę, punkty i struktury sieci, wykorzystywane systemy i aplikacje, jak i role personelu.
   - **Analiza Polityk i Procedur:** Analizujemy skuteczność polityk i procedur, aby upewnić się, że są zgodne z najlepszymi praktykami i wymogami regulacyjnymi.

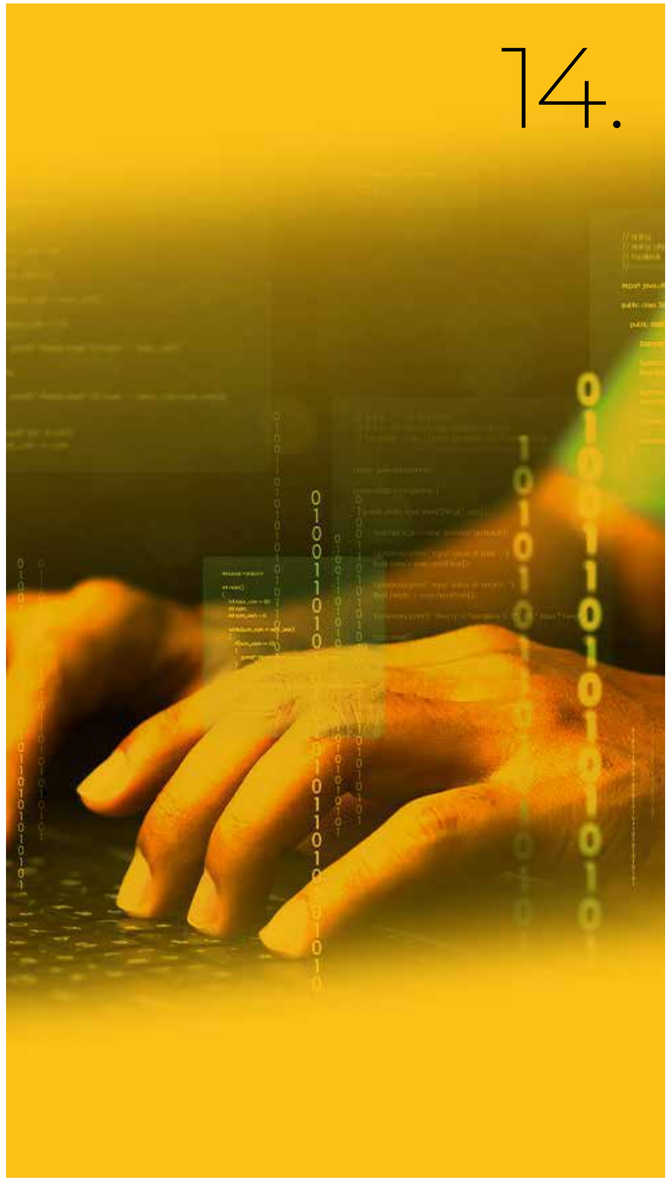
# SPERSONALIZOWANE PODEJŚCIE DO USŁUG

- **Skupienie na Skuteczności Kontroli i Ryzyku:** Priorytetem jest głęboka weryfikacja projektowania i skuteczności kontroli oraz podejście oparte na ryzyku, aby adresować specyficzne podatności i wymogi zgodności.
- **Monitorowanie i Dostosowanie:** Ciągle monitorujemy zmieniający się krajobraz zagrożeń i regulacji, aby zapewnić, że nasze podejście pozostaje aktualne i skuteczne w obliczu nowych wyzwań i technologii.
- **Skład Zespołu:** Dobieramy zespół z odpowiednimi umiejętnościami interdyscyplinarnymi, kompetencjami i doświadczeniem branżowym, aby dostosować się wymogów biznesowych i technologicznych. To zapewnia kompleksowe i w pełni profesjonalne podejście do adresowania wymagań Klientów.

# KOSZTY

- **Przejrzyste Ceny:** Koszty zależą od wielu czynników, takich jak branża, wielkość i złożoność, ale zapewniamy przejrzystość w naszym modelu cenowym. Będziesz rozumieć strukturę kosztów i wartość naszych usług.
- **Efektywność i Wartość:** Naszym celem jest dostarczanie maksymalnej wartości poprzez efektywną i skuteczną realizację usług. Dążymy do dostarczania rozwiązań kosztowo efektywnych, ale uwzględniających pełny profesjonalizm i najwyższą jakość.

14.



# NASZE PODEJŚCIE DO ZGODNOŚCI Z NIS 2.0 I UKSC

## NASZE SPERSONALIZOWANE PODEJŚCIE DLA KLIENTÓW IMPLEMENTUJĄCYCH NIS 2.0 I UKSC PO RAZ PIERWSZY

Przygotowanie organizacji do spełnienia wymagań NIS 2.0 i Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC) po raz pierwszy może być skomplikowanym i czasochłonnym zadaniem. Nasza firma wspiera organizacje, aby płynnie przejść przez ten proces za pomocą dostosowanego, trzyetapowego podejścia, zaprojektowanego w celu zapewnienia zgodności, wzmocnienia kontroli i ostatecznie zwiększenia wartości.

## ETAP 1 OCENA GOTOWOŚCI

**Cel:** Ocena obecnego stanu organizacji względem standardów NIS 2.0 i UKSC, identyfikacja luk lub braków w projektowaniu i skuteczności kontroli.

**Proces:** Zaczynamy od zaznajomienia Cię z wymaganiami NIS 2.0 i UKSC oraz określenia "luki zgodności" – obszarów, w których obecne praktyki są niewystarczające.

**Wynik:** Nasz szczegółowy raport zawiera te luki wraz z jasnymi rekomendacjami dotyczącymi ich naprawy.

**Czas trwania:** Około 6-8 tygodni.

Z naszych dotychczasowych doświadczeń wynika, iż obszarami, które często posiadają słabości są:

1. **Zarządzanie Podatnościami:** Brak proaktywnego podejścia do identyfikacji i łagodzenia podatności systemowych.
2. **Zarządzanie Konfiguracją i Utwardzaniem Systemu:** Systemy często są wdrażane z domyślnymi, niezabezpieczonymi konfiguracjami.
3. **Planowanie Ciągłości Działania (BCP)/Planowanie Odzyskiwania po Katastrofie (DRP):** Niewystarczające plany ciągłości działania i odzyskiwania po katastrofie.
4. **Niewystarczające Kontrole Dostępu:** Brak ścisłych kontroli nad tym, kto ma dostęp do wrażliwych danych i systemów.
5. **Niewłaściwe Procedury Zarządzania Zmianami:** Zmiany w systemach i oprogramowaniu są dokonywane bez odpowiedniego śledzenia lub testowania, co prowadzi do powstawania podatności.
6. **Brak Silnej Kultury Bezpieczeństwa:** Pracownicy często są najsłabszym ogniwem w cyberbezpieczeństwie z powodu braku świadomości i kompetencji.
7. **Niedostateczne Plany Reagowania na Incydenty:** Brak dobrze zdefiniowanego planu reagowania na incydenty cyberbezpieczeństwa.
8. **Niespójne Praktyki Szyfrowania Danych:** Wrażliwe dane często nie są odpowiednio szyfrowane, zarówno w spoczynku, jak i w trakcie przesyłania.
9. **Słabe Środki Ochrony Sieci:** Sieci są często niewystarczająco chronione przed zagrożeniami zewnętrznymi i wewnętrznymi.
10. **Nieaktualne lub Niezałatane Systemy:** Brak regularnych aktualizacji i łatek może pozostawić systemy podatne na nowe zagrożenia.
11. **Brak Kompleksowych Ocen Ryzyka:** Organizacje często pomijają regularne, kompleksowe oceny ryzyka.
12. **Nieskuteczne Zarządzanie Dostawcami:** Zewnętrzni dostawcy mogą nie przestrzegać standardów cyberbezpieczeństwa organizacji.
13. **Brak Dokumentacji Polityk i Procedur:** Polityki i procedury cyberbezpieczeństwa są nieudokumentowane lub nieaktualne.
14. **Brak Bezpiecznego Cyklu Życia Oprogramowania (SDLC):** Wiele organizacji nie integruje bezpieczeństwa w każdej fazie procesu tworzenia oprogramowania.
15. **Niewystarczające Monitorowanie Techniczne:** Brak ciągłego monitorowania systemów, infrastruktury i aplikacji, co prowadzi do opóźnionego wykrywania podatności i zagrożeń.

## ETAP 2 ZAMKNIĘCIE LUK

W Fazie 2 procesu zgodności, organizacja angażuje się aktywnie w zamykanie luk zidentyfikowanych podczas oceny gotowości. Ta faza jest kluczowa dla dostosowania praktyk do standardów NIS 2.0 i UKSC oraz przygotowania do audytu.

### Rozwój Planu Działania:

- **Na podstawie Wstępnych Rekomendacji:** Organizacja wykorzystuje nasze rekomendacje jako fundament do rozwiązania zidentyfikowanych wrażliwości i słabości.
- **Współpraca z Niezależnymi Doradcami:** Aby zachować integralność procesu audytu i unikać konfliktów interesów, możesz współpracować z zewnętrznymi, niezależnymi doradcami, którzy mogą dostarczyć dodatkowych wglądów i wskazówek.

### Odpowiedzialność Organizacyjna:

- **Wdrażanie Zmian:** Organizacja jest odpowiedzialna za integrację tych zmian w swoich wewnętrznych procesach. Ta faza jest kluczowa dla pełnego zrozumienia i internalizacji wymagań NIS 2.0 i UKSC.
- **Dostosowane Podejście:** Uznając unikalne aspekty organizacji, plan działania będzie dostosowany do specyficznych potrzeb i okoliczności.

### Czas Trwania i Skuteczne Rozwiązanie:

- **Ramy Czasowe:** Czas potrzebny na skuteczne zamknięcie tych luk będzie różny, w zależności od ich złożoności i wagi. Podkreślamy, że ważniejsze jest skuteczne rozwiązanie niż szybkość.

### Wspólny Wysiłek z Niezależnymi Ocenami:

- **Niezależna Współpraca:** Podczas gdy organizacja wewnętrznie jest odpowiedzialna za ten etap, wykorzystanie ekspertyzy niezależnych doradców może przynieść cenne wsparcie i zapewnić wszechstronne podejście do zgodności.
- **Zapewnienie Niezależności Audytu:** Taka współpraca wzmacnia obiektywny charakter nadchodzącego audytu, zapewniając brak konfliktów interesów.

## ETAP 3 AUDYT CYBERBEZPIECZEŃSTWA

Po zakończeniu początkowych przygotowań i zamknięciu luk, przechodzimy do fazy audytu zgodnego z NIS 2.0 i UKSC.
Ta faza obejmuje bardziej kompleksową i ciągłą ocenę środowiska kontrolnego organizacji przez określony okres.

### Audyt NIS 2.0 i UKSC:

- **Zakres:** Ten audyt ocenia zarówno odpowiednie zaprojektowanie kontroli, jak i ich operacyjną skuteczność zgodnie z wymaganiami zgodności.
- **Szczegółowe Sprawozdanie:** Audyt kończy się szczegółowym raportem odzwierciedlającym naszą niezależną i obiektywną opinię na temat zgodności. Oferuje on dogłębną analizę zaprojektowania i skuteczności kontroli.

**Szacowany Czas Trwania:**
Około 8-12 tygodni, w zależności od zakresu audytu.

**Minimalny Interwał:**
Obowiązkowy minimalny czas to 2 lata między audytami.

# NASZE ZAANGAŻOWANIE Z RÓŻNYMI KLUCZOWYMI FUNKCJAMI ORGANIZACJI

W procesie zgodności z NIS 2.0 i Ustawą o Krajowym Systemie Cyberbezpieczeństwa (UKSC) angażujemy się z różnymi kluczowymi funkcjami w Twojej organizacji, z szczególnym naciskiem na role związane z IT, HR, technologiami produkcyjnymi oraz ochroną fizyczną. Nasze podejście jest dostosowane, aby zapewnić kompleksowe pokrycie i dogłębne zrozumienie środowiska kontrolnego. Oto jak różnicujemy nasze zaangażowanie w zależności od funkcji organizacyjnych:

**SKUPIENIE NA KLUCZOWYCH FUNKCJACH ORGANIZACYJNYCH** Kluczowe Role i Departamenty:

1. **Chief Information Security Officer (CISO) i Chief Information Officer (CIO)/Chief Technology Officer (CTO)**
   - Odpowiedzialność za ogólne bezpieczeństwo IT, ochronę danych oraz zarządzanie technologią. Zapewnienie, że strategie IT i systemy są zgodne z wymaganiami NIS 2.0 i UKSC.
2. **Zespoły Administracji IT i Zabezpieczeń Sieci**
   - Skupienie na zabezpieczeniu sieci, szyfrowaniu danych i kontrolach dostępu. Zarządzanie i utrzymanie infrastruktury IT wspierającej operacje organizacji.
3. **Zespoły Rozwoju Oprogramowania i Inżynierii**
   - Ocena praktyk bezpiecznego tworzenia oprogramowania i bezpieczeństwa aplikacji. Zapewnienie, że wszystkie etapy cyklu życia oprogramowania (SDLC) zawierają elementy bezpieczeństwa.
4. **Zespoły ds. Zgodności IT i Zarządzania Ryzykiem**
   - Zrozumienie strategii zarządzania ryzykiem organizacji oraz zapewnienie zgodności z regulacjami. Implementacja i monitorowanie skuteczności kontroli ryzyka.

5. **Menedżerowie ds. Zasobów Ludzkich (HR)**
   - Ocena i wdrożenie kontroli związanych z zarządzaniem procedurami kadrowymi. Zapewnienie, że polityki bezpieczeństwa są skutecznie komunikowane i przestrzegane przez cały personel.

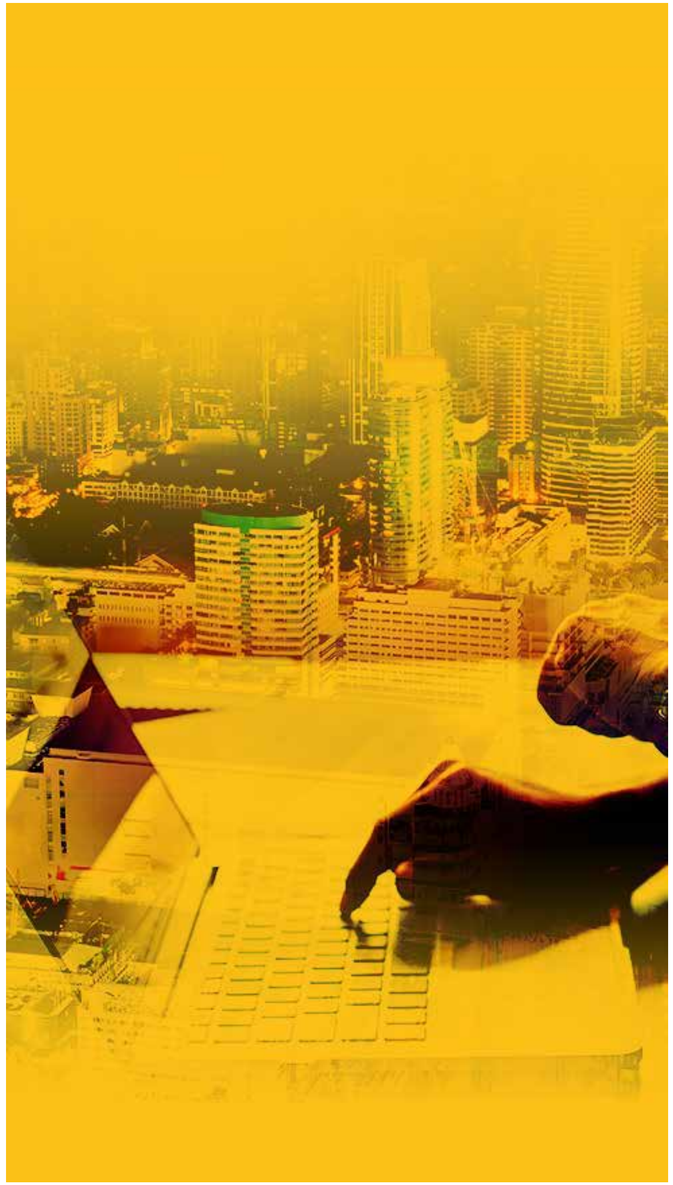
6. **Zespoły Odpowiadające za Technologie Produkcyjne (OT/ICS/SCADA)**
   - Zapewnienie bezpieczeństwa systemów kontrolnych i operacyjnych. Implementacja i monitorowanie środków ochrony specyficznych dla systemów przemysłowych, zgodnie z najlepszymi praktykami i standardami, takimi jak ISA/IEC 62443.

7. **Zespoły Ochrony Fizycznej**
   - Zapewnienie ochrony fizycznej infrastruktury. Ocena i wdrożenie środków bezpieczeństwa fizycznego, aby chronić przed nieautoryzowanym dostępem oraz innymi zagrożeniami fizycznymi.

8. **Menedżerowie Jednostek Biznesowych**
   - Dostarczanie operacyjnych spojrzenia na temat kontroli w swoich jednostkach.

9. **Zarząd i Najwyższe Kierownictwo**
   - Zaangażowanie jest kluczowe dla uzyskania holistycznego spojrzenia na zarządzanie, cele organizacyjne oraz praktyki zarządzania ryzykiem.

10. **Zespoły Zarządzania Dostawcami**
    - Szczególnie ważne dla zrozumienia zarządzania dostawcami zewnętrznymi i ich wpływu na środowisko kontrolne.



# NASZE PODEJŚCIE I CZAS TRWANIA AUDYTU

**Podejście:**

- Nasze podejście polega na dokładnym zrozumieniu i ocenie wewnętrznych polityk, procedur, kontroli oraz praktyk zarządzania ryzykiem w Twojej organizacji.
- Upewniamy się, że wszystkie istotne funkcje IT są kompleksowo ocenione.
- Polityki i procedury przechodzą szczegółową analizę, koncentrując się na porządku, organizacji, wewnętrznej spójności, przepływie danych oraz podziale obowiązków i odpowiedzialności.

**Nasze Zapewnienie:**

- **Spersonalizowana Usługa:** Uznając, że jedno podejście nie pasuje do wszystkich organizacji, nasze usługi są wysoce spersonalizowane w oparciu o unikalne cechy organizacji – profil ryzyka, oferowane usługi, otoczenie regulacyjne oraz wielkość organizacji.
- **Ekspert Zespół:** Nasi doświadczeni audytorzy przynoszą bogatą wiedzę w ocenie procesów biznesowych i systemów kontrolnych.
- **Jasna Komunikacja:** Utrzymujemy otwarte linie komunikacji przez cały proces audytu, zapewniając, że potrzeby i obawy są szybko adresowane.

# 15. BW ADVISORY SP. Z O.O.

## O nas

BW Advisory Sp. z o.o. to firma z ugruntowaną pozycją na rynku, specjalizująca się w nowoczesnych technologiach, bezpieczeństwie informacji oraz GRC (Governance, Risk Management, and Compliance) & Audyt z siedzibą główną w Polsce oraz biurami w Wielkiej Brytanii i Zjednoczonych Emiratach Arabskich. Jesteśmy liderem w dostarczaniu usług audytowych IT o najwyższej jakości, z doświadczonym 10-osobowym zespołem ekspertów operujących w różnych sektorach.

Nasze usługi obejmują pogłębione audyty SOC 1, SOC 2, SOC 3, a także inne audyty SOC w branżach takich jak finansowa, energetyczna i ICT. Specjalizujemy się w kompleksowych usługach bezpieczeństwa i audytu IT, kładąc szczególny nacisk na skuteczność systemów kontroli wewnętrznej i zarządzania ryzykiem. Oferujemy doradztwo przy wyborze i wdrożeniu systemów GRC, analizie przyczyn porażek biznesowych oraz dostarczamy kompleksową wiedzę o ryzykach dla organizacji. Nasza wiedza obejmuje także międzynarodowe standardy zgodności i cyberbezpieczeństwa, technical due diligence oraz cyfryzację ładu korporacyjnego w grupach kapitałowych, ze szczególnym uwzględnieniem ekspansji zagranicznej.

BW Advisory posiada bogate doświadczenie w realizacji zaawansowanych projektów dla sektora prywatnego i publicznego, pracując dla instytucji o wysokim profilu ryzyka oraz opracowując procedury bezpieczeństwa dla krytycznych instalacji. Nasza pasja do dzielenia się wiedzą skierowała nas również w stronę edukacji, prowadzimy akredytowane szkolenia i warsztaty. Nasze rozległe doświadczenie w audycie systemów IT/OT oraz znajomość specyfiki regulacyjnej rynków amerykańskich i europejskich pozwala nam skutecznie wspierać klientów w zgodności z wymogami prawnymi i zarządzaniu ryzykiem.

Nasze usługi obejmują również globalne usługi prywatności i zgodności IT oraz usługi zgodności i bezpieczeństwa AI, co pomaga organizacjom zarządzać wyzwaniami współczesnego rynku technologii i bezpieczeństwa.

# 16. NASZE KLUCZOWE PROJEKTY

1. **Doradztwo w Sektorze Lotnictwa Cywilnego:** Nasze doświadczenie obejmuje analizę i poprawę procedur bezpieczeństwa i ochrony w dużych projektach lotniczych, w tym opis procesów i analizę ryzyka dla zaawansowanego modelu statku powietrznego.
2. **Konsultacje w Sektorze Energetycznym:** Skutecznie doradzaliśmy i wdrażaliśmy wewnętrzne regulacje dla efektywności operacyjnej w instalacjach wysokiego ryzyka, szczególnie w branży gazowej, zgodnie ze ścisłymi standardami bezpieczeństwa ISRS.
3. **Analiza Przyczyn Porażek Biznesowych:** Przeprowadziliśmy innowacyjną i wielowymiarową analizę dla głównego podmiotu w sektorze energetycznym, wykorzystując narzędzia audytowe, techniki badania wypadków lotniczych i badania socjologiczne w celu identyfikacji głównych przyczyn porażek i rekomendowania ulepszeń.
4. **Audyty i Konsultacje Software Escrow dla Branży Finansowej:** Nasza wiedza obejmuje audytowanie i doradztwo w procesach software escrow dla oprogramowania branży finansowej, dostosowanego do rynku azjatyckiego.
5. **Szkolenia z Zarządzania Różnorodnymi Ryzykami:** Realizowaliśmy doradztwo i programu edukacyjne z zarządzania ryzykiem dla różnych sektorów, w tym finansowego, rozwojowego i energetycznego.
6. **Rozwój, Doradztwo i Wdrożenie Zintegrowanych Systemów GRC:** Nasze osiągnięcia obejmują projektowanie, doradztwo i wdrażanie zintegrowanych systemów GRC w firmach świadczących usługi medyczne i produkcyjne. Znacząco przyczyniliśmy się do rozwoju rynku GRC dla kilku wiodących firm oprogramowania i doradztwa.
7. **Zarządzanie Ciągłością Biznesu/Resiliency/Antifragility:** Audytowaliśmy, wdrażaliśmy i doradzaliśmy głównym grupom kapitałowym w sektorze energetycznym i rynkach wymiany energii z zakresu Systemów Zarządzania Ciągłością Działania.
8. **Rozwiązania w Zakresie Bezpieczeństwa Informacji i Cyberbezpieczeństwa:** Przeprowadziliśmy audyty, analizy i wdrożenia systemów bezpieczeństwa informacji i cyberbezpieczeństwa w różnych branżach, w tym branży finansowej, medycznej i energetycznej.
9. **Kompleksowe Audyty Bezpieczeństwa:** Nasze audyty bezpieczeństwa zapewniają zgodność z międzynarodowymi standardami w zakresie bezpieczeństwa informacji, cyberbezpieczeństwa i prywatności dla różnych globalnych organizacji.
10. **Wdrażanie Rozwiązań Zgodności:** Specjalizujemy się we wdrażaniu rozwiązań compliance związanych z ochroną danych, w tym RODO, prawem USA i Wielkiej Brytanii, a także politykami prywatności głównych firm technologicznych, w różnych sektorach IT.
11. **Implementacja SOC1 i SOC2 dla firmy gamingowej:** Wdrożono ramy ISO 27001, SOC1 finansowego, co umożliwiło firmie spełnienie międzynarodowych standardów bezpieczeństwa i zgodności.
12. **Implementacja SOC2 dla platformy AI SaaS dla firmy wellnes:** Przeprowadzono ocenę gotowości oraz wdrożono ramy prywatności i SOC2, w tym zgodność z przepisami prawnymi takimi jak RODO, HIPAA oraz wybranymi amerykańskimi przepisami stanowymi (CCPa, CPRA). Dodatkowo wdrożono wymagania zgodności z AI, zapewniając wysokiej jakości kontrole bezpieczeństwa, prywatności i odpowiedzialności algorytmów AI.
13. **Weryfikacja i opis mechanizmów kontroli IT dla grupy firm z branży spożywczej, w ramach oceny SOX 2002:** Przeprowadzono weryfikację oraz opis ogólnych mechanizmów kontroli IT zgodnie z wymaganiami SOX sekcja 404 oraz wymaganiami grupy i firmy matki notowanej na giełdzie w USA. Zapewniono zgodność z międzynarodowymi standardami oraz wymogami sprawozdawczości finansowej.

Nasze doświadczenie podkreśla nasze zaangażowanie w jakość, elastyczność i zdolność do dostarczania rozwiązań spełniających unikalne potrzeby naszych klientów na szybko zmieniającym się globalnym rynku. Wskazane portfolio wybranych projektów podkreśla nasze bogate doświadczenie i wszechstronność w obsłudze złożonych projektów i zadań wysokiego ryzyka w różnych sektorach. Cieszymy się z naszej zdolności do adaptacji i wyróżniania się w szeregu wymagających środowisk, dostarczając usługi doradcze, audytowe i wdrożeniowe najwyższej jakości.

# 17. LIDERZY

## SEBASTIAN BURGEMEJSTER

Sebastian ma ponad 15 lat doświadczenia w audycie wewnętrznym i zewnętrznym, wdrażaniu oraz zarządzaniu obszarami drugiej i trzeciej linii zapewnienia w organizacji. Posiada doświadczenie w implementacji, doradztwie i audytowaniu systemów zarządzania bezpieczeństwem informacji, zarządzaniem usługami IT, zarządzaniem ryzykiem oraz zarządzaniem jakością w różnych branżach i organizacjach, w tym międzynarodowych firmach z USA, UE, Wielkiej Brytanii i Australii.

Jest propagatorem zintegrowanej filozofii GRC, nowych technologii oraz intuicyjnego i zwinnego podejścia do zapewnienia bezpieczeństwa organizacji. Sebastian jest współtwórcą Antifragility Institute w Chicago, był prezesem i długoletnim członkiem zarządu Instytutu Audytorów Wewnętrznych IIA Polska, jest aktywnym członkiem AICPA, IIA, ISSA, ISACA oraz OCEG. Pełnił funkcję członka niezależnego w Komitecie Audytu Ministerstwa Spraw Zagranicznych oraz pracował w grupach roboczych ds. cyberbezpieczeństwa przy Ministrze Cyfryzacji.

Posiada prestiżowe międzynarodowe certyfikaty zawodowe, w tym CISA, CISM, CRISC, CDPSE, CCAK, CCSA, CGAP, CRMA, LA ISO27001, LA ISO20000, CSXF, ACE, GRCP, GRCA, COBIT2019F, COSO Internal Control, Advanced SOC, Cybersecurity Advisory Services, SOC for cybersecurity, SOC for supply chain oraz jest akredytowanym trenerem ISACA.

## PIOTR WELENC

Piotr Welenc to doświadczony profesjonalista z ponad 25-letnim doświadczeniem w branży IT, audycie wewnętrznym i zewnętrznym. Posiada bogate doświadczenie zawodowe, zdobyte w pracy dla największych instytucji finansowych i prawnych w Polsce i Europie. Piotr specjalizuje się w audycie wewnętrznym i IT, a jego wiedza ekspercka obejmuje również zarządzanie ryzykiem, optymalizację procesów, zarządzanie korporacyjne i IT, zgodność oraz ustawę Sarbanes-Oxley z 2002 roku (SOX). Pełnił funkcje przewodniczącego/członka Rady Nadzroczej lub doradcy w spółkach notowanych na GPW w zakresie GRC oraz ESG.

Piotr jest współautorem systemów IT wspierających procesy GRC w spółkach notowanych na GPW oraz instytucjach opieki zdrowotnej, pierwszego systemu klasy GRC w Polsce, który cyfryzował procesy w firmach. Poza rolami zawodowymi Piotr jest zaangażowanym edukatorem, wykładającym na studiach podyplomowych z zakresu audytu wewnętrznego, IT, zarządzania ryzykiem oraz aktywnie uczestniczącym w grupach roboczych ds. cyberbezpieczeństwa przy Ministerstwie Cyfryzacji.

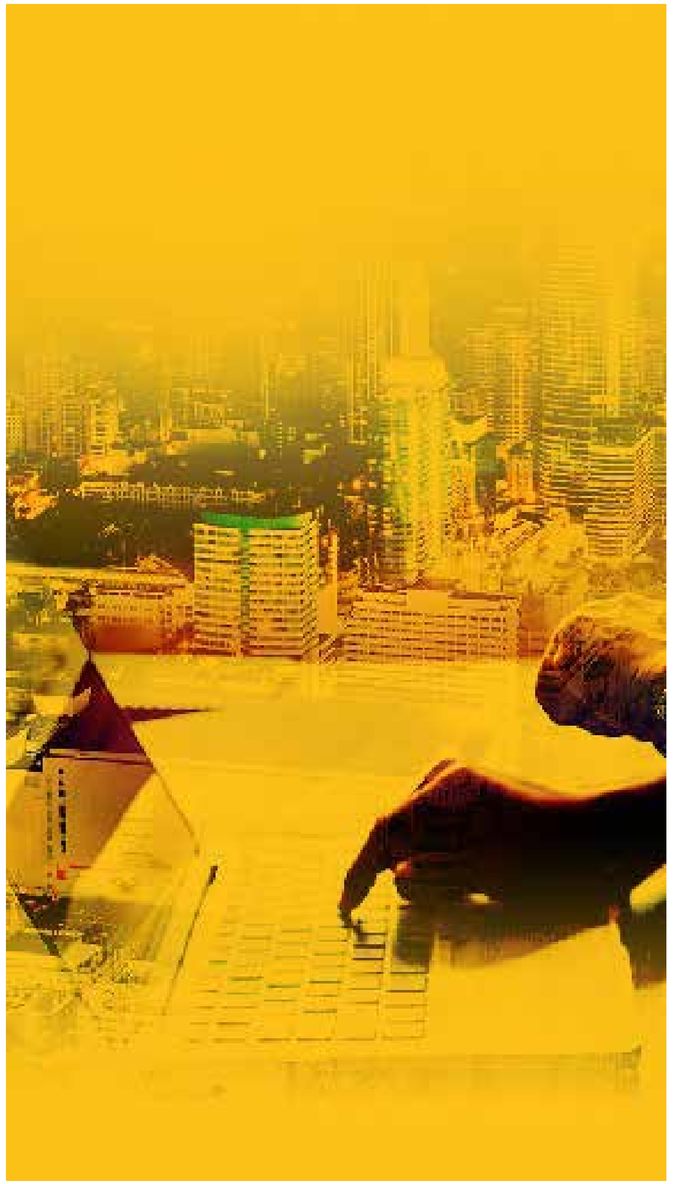
Ponadto Piotr jest współzałożycielem Instytutu Antifragility w Chicago, kładącego nacisk na innowacje i odporność. Posiada kolekcję prestiżowych międzynarodowych certyfikatów zawodowych, w tym MBA, CISA, CICA, CGEIT, CRISC, CDPSE, CRMA, ACO, AESGO, QAVal., ISO22301 LA, ISO27001 LA i ISO20000 LA. Jako akredytowany trener ISACA, kontynuuje wkład w rozwój zawodowy innych.

18.

# NASZE GŁÓWNE USŁUGI

**Usługi w Zakresie Cyberbezpieczeństwa i Bezpieczeństwa Informacji:**

- **Bezpieczeństwo Organizacyjne i Odporność Cybernetyczna:** Tworzenie kompleksowych strategii dla bezpieczeństwa i odporności na poziomie organizacyjnym.
- **Zgodność z Cyberbezpieczeństwem i Jej Wzmacnianie:** Dostosowywanie systemów cyberbezpieczeństwa do kluczowych przepisów tj. Dyrektywy NIS2, DORA, CER, ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), rekomendacjami i wytycznymi KNF oraz standardami międzynarodowymi m.in. ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 22301, NIST, FedRAMP, TSC dla SOC2, CCM.
- **Zgodność z Wymaganiami Prywatności i Ochrony Danych Osobowych:** Wdrażanie i wzmacnianie systemów ochrony danych osobowych w oparciu o Europejskie i Międzynarodowe wymagania, tj. RODO, UK GDPR, CCPA/CPRA, COPPA, HIPPA oraz wymagania korporacyjne np. Microsoft SSPA, tj. w celu zapewnienia zgodności.
- **Usługi Zarządzania Ryzykiem Strony Trzeciej (TPRM):** Specjalizujemy się w ocenie i zarządzaniu ryzykiem związanym z bezpieczeństwem informacji, odpornością organizacyjną i ochroną danych osobowych przy współpracy ze stronami trzecimi. Nasze działania obejmują kompleksową analizę i audyty zgodności z międzynarodowymi standardami, zapewniając przestrzeganie najlepszych praktyk w zakresie bezpieczeństwa informacji i ograniczenie ryzyka dlaklienta końcowego.
- **Usługi Wirtualne:** Oferowanie wirtualnych ról takich jak Dyrektor ds. Bezpieczeństwa Informacji (CISO), Inspektor Ochrony Danych (DPO), Oficer ds. Zgodności (CCO), Oficer ds. Ryzyka (CRO) oraz Oficer ds. Ryzyka w Łańcuchu Dostaw (CSCRO) dla elastycznego, eksperckiego wsparcia organizacji.
- **Zaawansowane Audyty Cyberbezpieczeństwa:** Specjalizacja w kompleksowych audytach IT, bezpieczeństwa informacji i cyberbezpieczeństwa, zaprojektowanych do rygorystycznej oceny systemów zgodnie ze standardami branżowymi i wymogami regulacyjnymi np. KSC.



## Usługi Technologiczne i Innowacyjne:

- **Integracja Zaawansowanych Technologii:** Oferowanie strategicznego projektowania funkcji IT, zarządzania i doradztwa, ze szczególnym uwzględnieniem nowych technologii takich jak AI, ML, IoT.
- **Strategia Blockchain i Metaverse:** Zapewnianie eksperckiego doradztwa w zakresie integracji technologii blockchain i metaverse w celu optymalizacji efektywności operacyjnej i budowania przewagi konkurencyjnej.
- **Strategia IT i Zarządzanie Usługami:** Doradztwo w zakresie strategii IT (COBIT2019) i ram zarządzania usługami (ISO 20000, ITIL).
- **Technical due dilligence (techniczny due diligence):** Zewnętrzna profesjonalna i obiektywna ocena poziomu technicznego, IT i bezpieczeństwa podmiotów gospodarczych, w szczególności w trakcie procesu zakupu / finansowania..

## Usługi Zarządzania, Ryzyka i Zgodności (GRC):

- **Zintegrowane Rozwiązania GRC i IT GRC:** Dostarczanie kompleksowych rozwiązań w obszarze Ładu, Ryzyka i Zgodności oraz specyficznych wyzwań IT GRC.
- **Rozwój Systemów Compliance:** Budowanie i rozwijanie systemów zgodności, ze szczególnym naciskiem na ochronę prywatności i zarządzanie ryzykiem operacyjnym.
- **Wzmocnienie Zarządzania Ryzykiem i Odpornością:** Poprawa ram zarządzania ryzykiem i governance w celu zwiększenia odporności i dojrzałości organizacji.

## Kompleksowe Usługi Audytu i Zapewnienia:

- **Specjalistyczne Usługi Audytowe:** Prowadzenie szeregu specjalistycznych audytów, w tym ISAE 3402, SSAE16, SOC 1, 2, 3, koncentrujących się na różnych aspektach operacyjnych i zgodności.
- **Kompleksowy Audyt IT:** Oferowanie szczegółowych audytów IT, badających skuteczność, bezpieczeństwo i odporność infrastruktury IT, zapewniając ich zgodność z celami biznesowymi i wymogami zgodności.
- **Dogłębny Audyt Cyberbezpieczeństwa:** Wykonanie audytów cyberbezpieczeństwa, ocena adekwatności i skuteczności zabezpieczeń cyberbezpieczeństwa, identyfikacja luk i dostarczanie praktycznych wskazówek do wzmacniania bezpieczeństwa.
- **Audyt Ciągłości Działania:** Prowadzenie audytów planów ciągłości działania w celu zapewnienia, że są one kompleksowe, skuteczne i zgodne z najlepszymi praktykami i standardami.
- **Niezależne Usługi Zapewnienia i Doradztwa:** Dostarczanie specjalistycznych, bezstronnych ocen i konsultacji, mających na celu podniesienie jakości i bezpieczeństwa operacji biznesowych.

## AI Compliance i Zarządzanie:

- **Ocena Zgodności z AI:** Przeprowadzamy szczegółowe oceny zgodności z międzynarodowymi standardami AI, takimi jak ISO/IEC 42001, NIST AI Risk Management Framework oraz wytyczne OECD dotyczące AI oraz regulacjami, w tym EU AI Act, DCIA, RODO i CCPA.
- **Zarządzanie Ryzykiem AI:** Oferujemy wsparcie w zarządzaniu ryzykiem związanym z AI, w tym ocenę ryzyka, identyfikację luk oraz rozwój strategii zarządzania ryzykiem.

## Ochrona Prywatności i Bezpieczeństwo AI:

- **Zarządzanie Danymi i Prywatnością:** Pomagamy w implementacji technologii ochrony prywatności, takich jak anonimizacja danych i prywatność różnicowa, w celu zapewnienia zgodności z regulacjami ochrony danych osobowych.
- **Bezpieczeństwo Systemów AI:** Zapewniamy wsparcie w tworzeniu bezpiecznych systemów AI, obejmujące mechanizmy obronne przeciwko atakom adwersarialnym oraz zabezpieczenia systemów AI zgodnie z najlepszymi praktykami branżowymi.

## Zarządzanie i Udoskonalanie AI:

- **Ciągłe Monitorowanie i Doskonalenie:** Oferujemy usługi ciągłego monitorowania i doskonalenia systemów AI, aby zapewnić ich zgodność z najnowszymi regulacjami i standardami technologicznymi.
- **Audyt i Certyfikacja AI:** Przeprowadzamy audyty zgodności AI oraz przygotowujemy do certyfikacji, takich jak SOC2+ oraz ISO/I EC 42001, zapewniając pełną zgodność z wymogami regulacyjnymi oczekiwaniami klientów.

## Usługi z Zakresu ESG (Environmental, Social, Governance):

- Integracja aspektów środowiskowych, społecznych i zarządzania w strategię firmy.
- Doradztwo i wdrażanie praktyk zrównoważonego rozwoju.
- Analiza i ocena wpływu działalności firmy na środowisko i społeczność.
- Wspieranie transparentności i odpowiedzialności korporacyjnej.
- Audyt przygotowania do spełnienia wymogów ESG.

## Strategiczne Zarządzanie i Doskonałość Operacyjna:

- **Konsultacje Biznesowe i IT:** Pomoc w opracowaniu i wdrożeniu spójnych i przyszłościowych strategii biznesowych i IT.
- **Zarządzanie Kosztami i Przygotowanie do Certyfikacji ISO:** Doradztwo dla organizacji w zarządzaniu kosztami i przygotowaniu do certyfikacji ISO, zapewniając zgodność z międzynarodowymi standardami.

Nasza oferta obejmuje kompleksowe usługi dostosowane do potrzeb każdej organizacji, pomagając im osiągnąć wyznaczone cele strategiczne, operacyjne i technologiczne, a także zapewnić zgodność z obowiązującymi przepisami oraz zasadami ESG.

# 19. NASZE KOMPETENCJE

# 20. JESTEŚMY CZŁONKAMI

## WIELU MIĘDZYNARODOWYCH I KRAJOWYCH INSTYTUCJI

The Institute of Internal Auditors

The Institute of
Internal Auditors

OCEG

Open Compliance and
Ethics Group

ISACA

Information Systems
Audit and Control Association

Instytut Compliance

Compliance Institute

#Cyber Made InPoland

Cyber Made In Poland Cluster

Viadrina Compliance Center

Viadrina Compliance Center

ISSA Information Systems Security Association

Information Systems
Security Association

Association of International Certified Professional Accountants

Association of International
Certified Professional Accountants

iapp

International Association
of Privacy Professionals

PFSz Polska Federacja Szpitali

Polish Hospital Federation

CSA cloud security alliance®

Cloud Seciurity Alliance