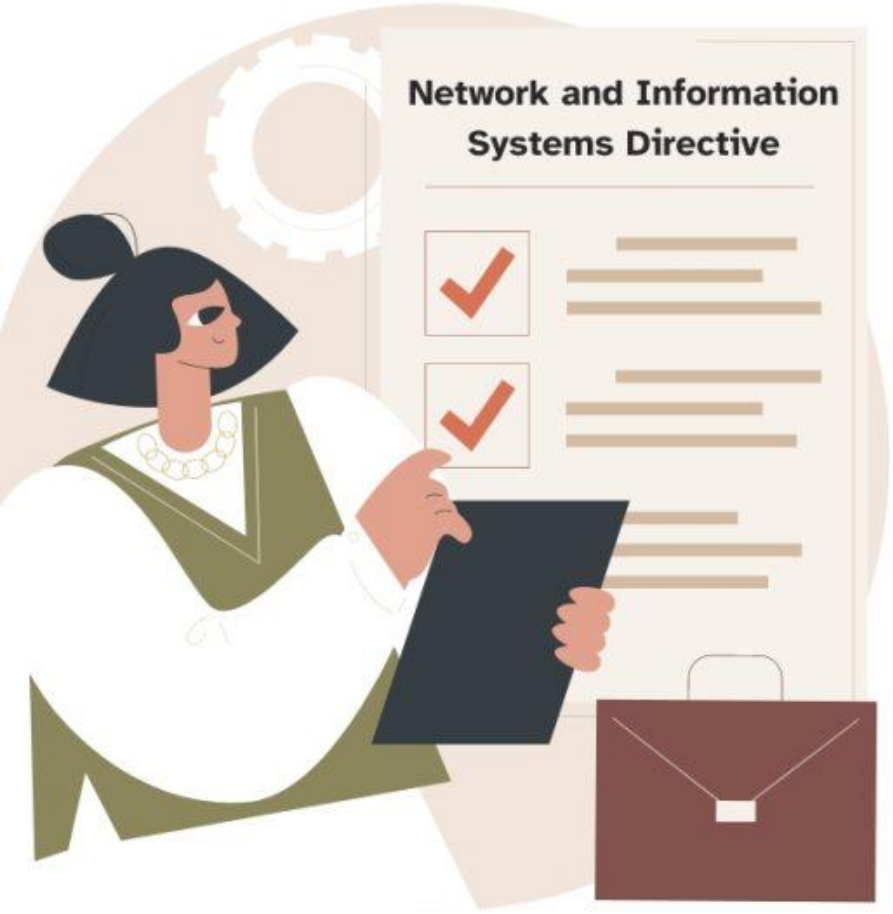
# Dlaczego NIS2 kosztuje tak dużo? Założenie, wdrożenie, informowanie, reagowanie.

Andrzej Piotrowski (ITAudit,ISSA Polska, ISACA Polska)




## Dyrektywa NIS2

NIS2 (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555) została opublikowana 14 grudnia 2022 r. a jej termin implementacji 2 upływa 17 października 2024 r. Podobnie jak DORA, NIS2 ma na celu zwiększenie odporności cyfrowej kluczowych sektorów gospodarki, jednak skupia się na szerszym spektrum sektorów, nie tylko finansowych. W przypadku NIS 2, odpowiedzialność spoczywa również na zarządach organizacji, które muszą zatwierdzać polityki bezpieczeństwa, monitorować ich przestrzeganie oraz podejmować działania w celu zarządzania ryzykiem.

# Ustawa o krajowym systemie cyberbezpieczeństwa

## Perspektywa administracji rządowej

Autor dokumentu: Departament Komitetu do Spraw Europejskich , wprowadzony przez: Magdalena Grymla-Bednarczyk
Data utworzenia: 11-12-2024

KSE TR. POTW. 2024-12-10_Projekt ustawy_UC32 - uwagi MS po terminie.pdf
Autor dokumentu: Departament Komitetu do Spraw Europejskich , wprowadzony przez: Magdalena Grymla-Bednarczyk
Data utworzenia: 11-12-2024

KSE TR. POTW. 2024-12-10_Projekt ustawy_UC32 - uwagi MRiT po terminie.pdf
Autor dokumentu: Departament Komitetu do Spraw Europejskich , wprowadzony przez: Magdalena Grymla-Bednarczyk
Data utworzenia: 13-12-2024

Pismo Prezesa PIKE dot. braków w OSR uKSC.pdf
Autor dokumentu: Departament Komitetu do Spraw Europejskich , wprowadzony przez: Agnieszka Mróz
Data utworzenia: 19-12-2024

Pismo Prezesa PIKE 1. raport FCC.pdf
Autor dokumentu: Departament Komitetu do Spraw Europejskich , wprowadzony przez: Agnieszka Mróz
Data utworzenia: 19-12-2024

Pismo Prezesa PIKE 4. raport FCC.pdf
Autor dokumentu: Departament Komitetu do Spraw Europejskich , wprowadzony przez: Agnieszka Mróz
Data utworzenia: 19-12-2024

Pismo Prezydenta Konfederacji Lewiatan.pdf
Autor dokumentu: Departament Komitetu do Spraw Europejskich , wprowadzony przez: Agnieszka Mróz
Data utworzenia: 23-12-2024

KSE TR. POTW 2025-02-13 - Tekst ostateczny 2 - RCL - uwagi.pdf
Autor dokumentu: Departament Komitetu do Spraw Europejskich , wprowadzony przez: Agnieszka Mróz
Data utworzenia: 14-02-2025

sienie się wnioskodawcy do uwag

nia Komitetu Data ostatniej modyfikacji: 13-02-2025

KSE 2025-02-13 Komunikat ws. przyjęcia dokumentu_UC32.pdf
Autor dokumentu: Departament Komitetu do Spraw Europejskich , wprowadzony przez: Agnieszka Mróz
Data utworzenia: 13-02-2025

Rekomendacja SKRM_Projekt ustawy_UC32.pdf
Autor dokumentu: Departament Komitetu do Spraw Europejskich , wprowadzony przez: Agnieszka Mróz
Data utworzenia: 13-02-2025

ISSA POLSKA

itaudit

**Za naruszenie obowiązków czekają liczne sankcje.**

*„Podmiot zagrożony karą administracyjną w gorszej sytuacji prawnej, aniżeli miałby ją w przypadku zagrożenia sankcją prawa karnego. Ważkie wątpliwości rodzi obciążanie administracyjną karą pieniężną nie tylko podmiotu kluczowego czy podmiotu ważnego, ale również osoby fizycznej – kierownika podmiotu kluczowego/ważnego. Pociąganie osoby fizycznej do odpowiedzialności administracyjnej o charakterze majątkowym (pieniężnym), niezależnie od zawinienia....”*

# Koszty wdrożenia i reagowania na incydenty bezpieczeństwa (cyberatak)

**Nowe procesy bezpieczeństwa**

•Kluczowe dla minimalizacji ryzyka ataku.

•Wymagane przez NIS2: m.in. system zarządzania ryzykiem, polityka bezpieczeństwa, monitoring incydentów.

**Nowe technologie**

•SIEM (Security Information and Event Management).

•Systemy EDR/XDR (Endpoint Detection & Response).

•Segmentacja sieci, szyfrowanie, kopie zapasowe.

**Szkolenia i rozwój zespołu**

•Pracownicy muszą rozumieć zagrożenia i procedury bezpieczeństwa.

•Koszt związany z regularnymi szkoleniami personelu

•Osobne szkolenie dla zarządu

itaudit

***Nowa (Piąta) Nowelizacja o Krajowym Systemie Cyberbezpieczeństwa – nowości o karach***

*Dodatkowa kara finansowa do 100 mln zł.*

……

*Przypadek ekstremalny, który spowoduje narażenie kraju na zagrożenia cyberbezpieczeństa obronności, zdrowia życia ludzi.*

…….

*Dodatkowo na podmioty kluczowe jak i ważne mogą być nakładane kary pieniężne administracyjne*

…….

*Podmiot który opóźnia się w wykonaniu realizacja postanowienia ma mieć zasadzoną karę która będzie wynosić od 50 to do 100 tys zł za każdy dzień opóźnienia, liczona od końcowej daty wykonania wszystkich prac które*

# Dlaczego NIS2 generuje koszty?

## Trzy główne obszary kosztów

Koszty wdrożenia nowych procedur i systemów.

Koszty gotowości na incydenty i reagowania na ataki.

Koszty długoterminowego utrzymania zgodności.

## NIS2 to nie tylko regulacja, ale realne koszty

Wdrożenie NIS2 wymaga inwestycji w technologie (sprzęt i oprogramowanie) ale również wdrożone procesy i zasoby ludzkie (przeszkolone).

## Przykład wyliczeń na średniej firmy wpisanej na listę podmiotów pod NIS2

Na listę można trafić na wiele sposobów, obecnie mówi się o ok 90-100 tys podmiotów które będą wpisane na liście jak podmioty podlegające

itaudit

# Koszt narzędzi – zakup (bez utrzymania)

**1.Systemy Zarządzania Bezpieczeństwem Informacji (ISMS) Koszt**: 10 000 - 50 000 zł.
**Opis**: Oprogramowanie do zarządzania politykami bezpieczeństwa, audytami i dokumentacją.
**2.Systemy Wykrywania i Zapobiegania Włamaniom (IDS/IPS) Koszt**: 15 000 - 100 000 zł.
**Opis**: Oprogramowanie do monitorowania ruchu sieciowego i wykrywania potencjalnych zagrożeń.
**3.Rozwiązania do Monitorowania Bezpieczeństwa (SIEM) Koszt**: 20 000 - 200 000 zł.
**Opis**: Oprogramowanie do zbierania, analizowania i raportowania incydentów.
**4.Zarządzanie Tożsamością i Dostępem (IAM) Koszt**: 10 000 - 60 000 zł.
**Opis**: Oprogramowanie do zarządzania dostępem użytkowników
**5.Szyfrowanie Danych Koszt**: 5 000 - 30 000 zł.
**Opis**: Oprogramowanie do szyfrowania danych w spoczynku i w transmisji.

**Koszty Infrastruktury - zakup (bez utrzymania)**
**1.Serwery i Sprzęt Sieciowy Koszt**: 30 000 - 200 000 zł.
**Opis**: Zakup serwerów, zapór sieciowych
**2.Usługi Chmurowe Koszt**: Zależny od dostawcy, średnio od 500 zł/miesiąc do kilku tysięcy złotych rocznie.

**A gdzie obsługa (Ludzie) i Wdrożenie (Ludzie) i Szkolenia (Ludzie) i na końcu Utrzymanie.**

**A to nie wszystkie koszty... bo incydent może powstać w każdej chwili....**


## Od czego zaczyna się historia incydentu

.....w godzinach wieczornych został przeprowadzony atak hakerski (typu ransomeware), który doprowadził do naruszenia ochrony danych osobowych poprzez atak złośliwego oprogramowania szyfrującego pliki przechowywane na naszych serwerach.

## Jakie dane osobowe obejmowało naruszenie?

W szczególności zdarzenie obejmuje następujące dane: imię i nazwisko, dane teleadresowe (w tym adres email oraz nr telefonu jeżeli były podawane), dane związane z załatwianą sprawą (np. dane zawarte na wniosku, dane na fakturze w przypadku dokonywania opłat).

*Naruszenie dotyczyło danych z systemu m.in. programu do elektronicznego obiegu dokumentów oraz programów związanych z wystawianiem dokumentów księgowych w związku z czym naruszenie dotyczy petentów załatwiających swoje sprawy w ...” – stwierdzono w pewnej firmie ze Szczecina*

RADIO SZCZECIN

itaudit

***A jakie obowiązki czekają na kierowników podmiotów ważnych i kluczowych?***

*„Kierowników tych podmiotów i zarządy spółek czeka sporo żmudnej interdyscyplinarnej pracy wymagającej zespołów informatyków, prawników itd. Projektodawca określa obowiązki podmiotów kluczowych i ważnych w zakresie wdrażania systemu zarządzania bezpieczeństwem informacji, który musi obejmować szacowanie ryzyka, wdrażanie odpowiednich środków ochrony, monitorowanie zagrożeń oraz zarządzanie incydentami. „*

*„Zmniejszenie maksymalnego wymiaru kary finansowej dla kierowników podmiotów kluczowych i ważnych, z 600 do 300% wynagrodzenia.”*

# Konsekwencje operacyjne nie spełnienia wymogów UoKSC (NIS2)

**Jakie kary przewiduje NIS2?**

Zgodnie z artykułem 34 i 35 dyrektywy NIS2, instytucje publiczne i podmioty prywatne, które nie spełniają wymogów w zakresie cyberbezpieczeństwa, mogą być obciążone następującymi sankcjami:

**Kary finansowe**

•Dla podmiotów **„Essential”** (podstawowych, **kluczowych** – np. usługi komunalne):

- Do 10 mln EUR lub 2% rocznego światowego obrotu **W przypadku „Firma ze  Szczecin”, przy założonym zysku netto 69 mln zł (~15,5 mln EUR), kara mogłaby wynieść maksymalnie 10 mln EUR (ok. 50 mln zł).**

•Dla podmiotów **„Important”** (**ważnych**, ale mniej krytycznych):

- Do 7 mln EUR lub 1,4% rocznego światowego obrotu.

itaudit

## **Kary obecne w ustawie o krajowym system cyberbezpieczeństwa (**Artykuł 73 UoKSC)

| Rodzaj naruszenia | Maksymalna kara (PLN) |
|---|---|
| **Brak zgodności z wymogami KSC** | 150 000 zł |
| **Nieprzekazanie informacji o zabezpieczeniach** | 100 000 zł |
| **Brak współpracy z organem nadzoru** | 50 000 zł |
| **Brak planu zarządzania incydentami** | 15 000 zł |
| **Brak realizacji obowiązków podmiotu kluczowego** | 50 000 zł |
| **Nieobsłużenie incydentu** | 15 000 zł za każdy przypadek |
| **Brak zgłoszenia incydentu poważnego** | 20 000 zł za każdy przypadek |
| **Brak zgłoszenia incydentu istotnego** | 20 000 zł za każdy przypadek |
| **Nieprzekazanie raportu po incydencie** | 20 000 zł |
| **Brak wdrożenia zaleceń organu nadzoru** | 100 000 zł |
| **Zaniechanie wdrożenia środków naprawczych** | 200 000 zł |
| **Brak przeprowadzenia audytu bezpieczeństwa** | 50 000 zł |

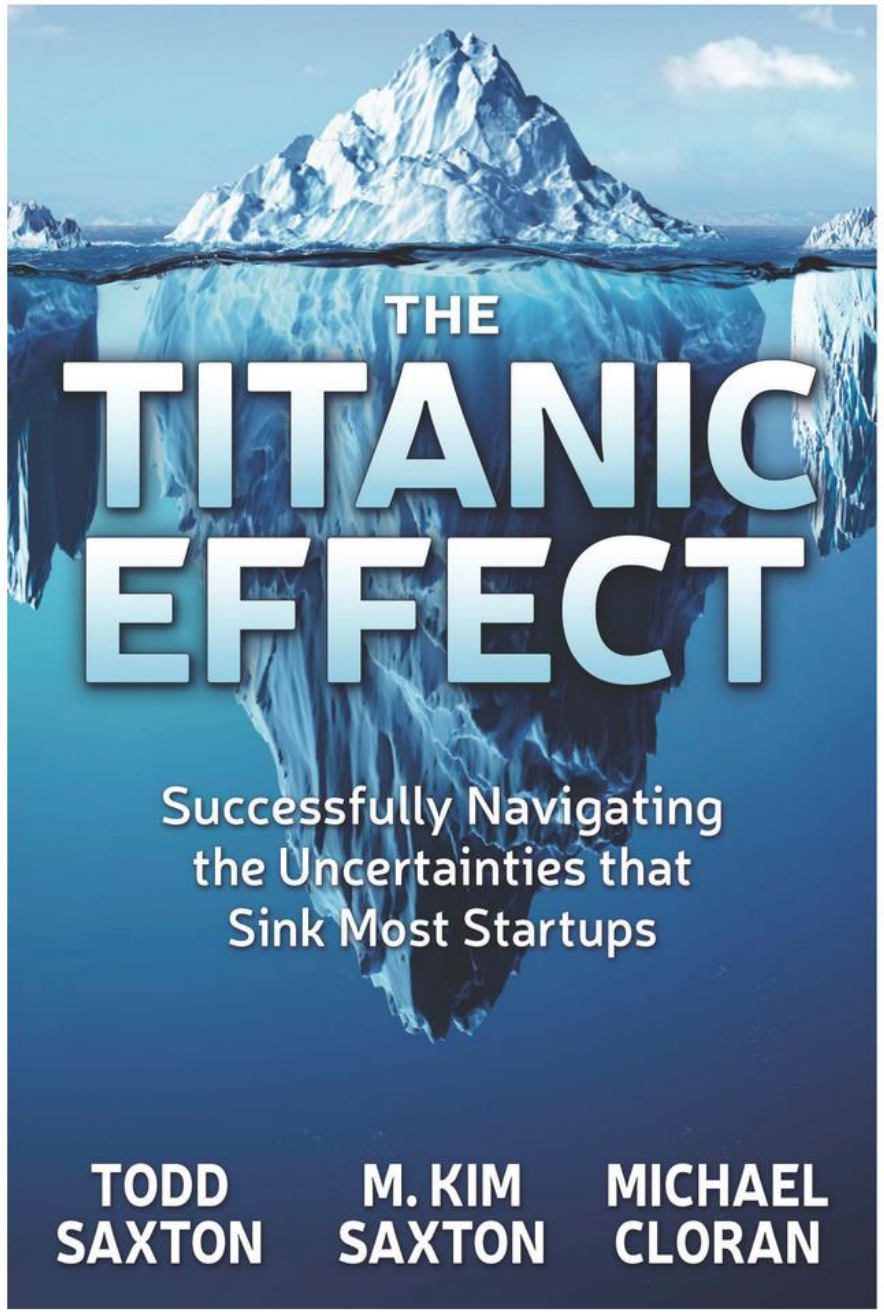
## **A kiedy to zacznie obowiązywać bo NIS2 nie obowiązuje w Polsce – Nas rozlicza UoKSC ? Prawda....**

**W Polsce NIS2 obowiązuje od 17 Października 2024** na terenie całej Unii Europejskiej...

Spodziewamy się, że projekt nowelizacji KSC trafi do Sejmu na przełomie **marca** i **kwietnia**. Określony w niej aktualnie okres vacatio legis to **jeden miesiąc** od dnia ogłoszenia.


**Dodatkowe informacje znajdą Państwo na stronie Ministerstwa Cyfryzacji**

itaudit



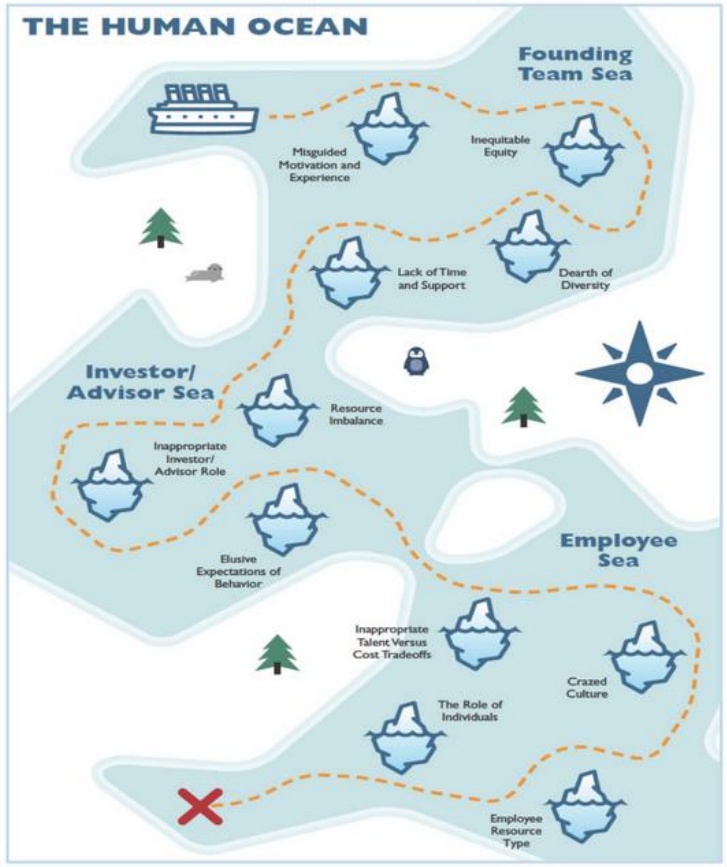

Analiza Ryzyka

Analiza Zagrożeń

Ciągłość Działania

Wymagane Dokumenty

~~Navigation Map~~




Reagowania na Incydenty

Plan Ciągłości Działania

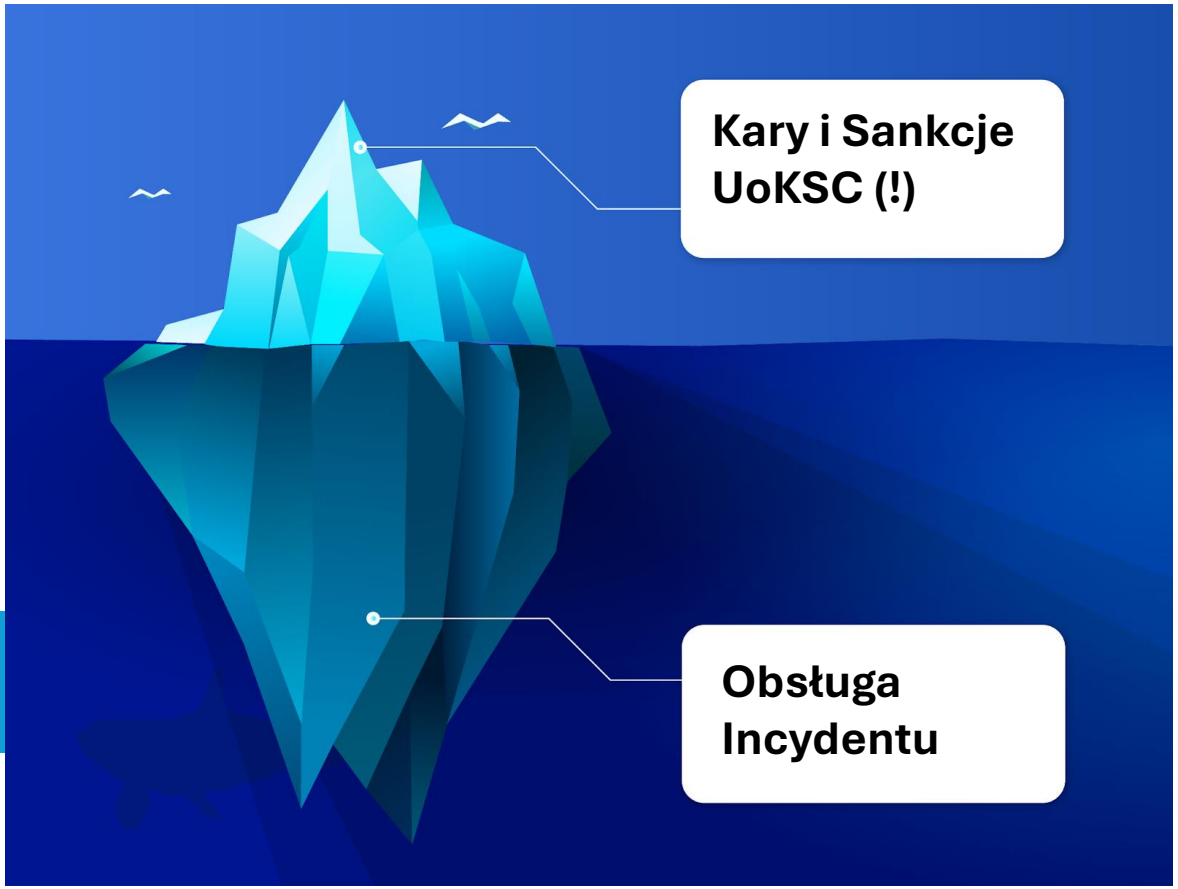
Rejestr Zgłoszeń Incydentów

Dokumentacja Techniczna

~~Iceberg Index~~

| Founding Team Sea | | Strong – Smooth Sailing | Some – Rocky Journey Ahead | Very Little – Need a Navigation Plan | Not At All – Large Debilitergs In Sight |
|---|---|---|---|---|---|
| **Misguided Motivation and Experience** | Founding team has:<br>• Passion for solving this problem<br>• Experience with the problem<br>• Persistence to overcome hurdles<br>• Ability to listen to feedback | ☐<br>☐<br>☐<br>☐ | | | |
| **Inequitable Equity** | Vesting plan:<br>• Allocates equity over time<br>• Is based on contribution<br>• Has a future set aside | ☐<br>☐<br>☐ | | | |
| **Dearth of Diversity** | Founding team has diverse perspectives:<br>• Industry experience<br>• Technological competence<br>• Functional backgrounds<br>• Cultural backgrounds | ☐<br>☐<br>☐<br>☐ | | | |

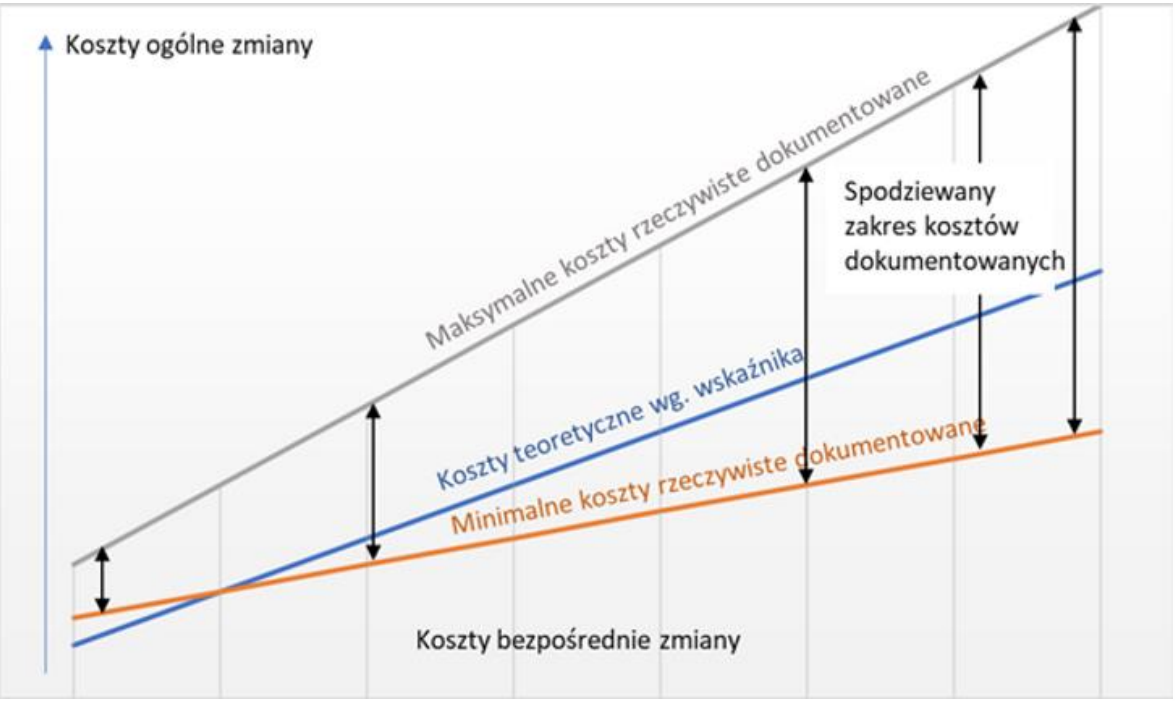
itaudit

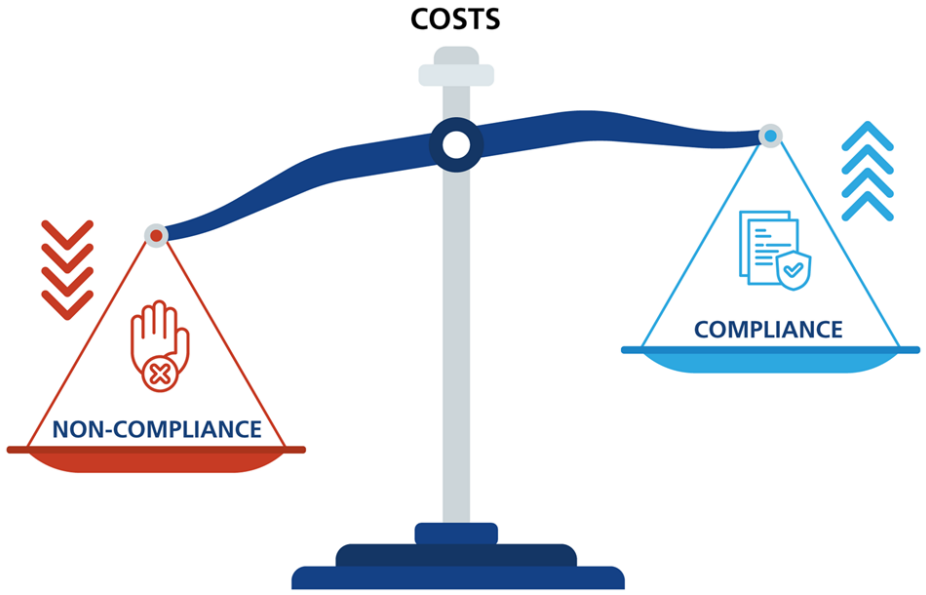



# Jak zoptymalizować koszty wdrożenia NIS2?

- Outsourcing SOC’a
- Przygotowanie Polityk i Procedur wraz z vCISO
- Szkolenia i Audyty


| | I / Rok 1 | vs budżet | | I / Rok 1 | vs budżet |
|---|---|---|---|---|---|
| EBITDA | 81 028 | +7421 +10,1% | Przychody netto projekty | 156 000 | +23400 +17,6% |
| Przychody netto | 250 920 | +5761 +2,3% | Przychody netto handel | 82 920 | -8080 -8,9% |
| Marża EBITDA | 32,3% | +2,3p.p. +7,6% | Przychody netto pozostałe | 12 000 | -9559 -44,3% |
| **Kluczowe Wskaźniki Efektywności** | | | | | |
| ROE | 7,3% | +0,8p.p. +12% | Środki pieniężne | 14 971 | +3071 +25,8% |
| Przepływy z dział. oper. | -197 615 | -19761 -11,1% | Zadłużenie netto | -235 029 | -7029 -3,1% |




# Kiedy NIS2 kosztuje "za dużo"?

**Czy istnieje „próg opłacalności” compliance?**

**•Tak! Koszty compliance powinny być niższe niż potencjalne straty.**

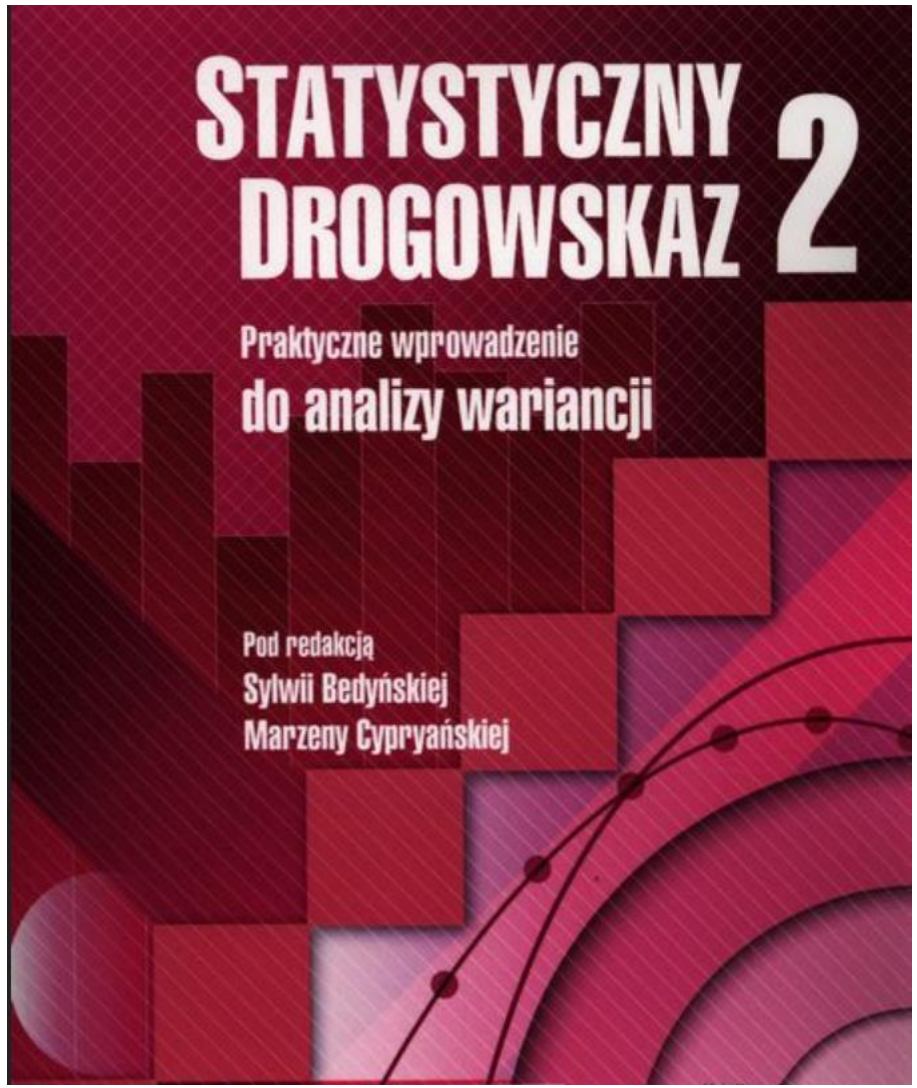
**•A ta Firma ze Szczecina miała przecież wszystko?**

Brak wystarczających inwestycji w prewencję → **konsekwencje finansowe i reputacyjne**.

**Jak zoptymalizować koszty?**

- **Szkolenia i Cyberhigiena – na wielu poziomach i zasadach działania**.
- **Zarządzanie ryzykiem** – identyfikacja kluczowych obszarów wymagających ochrony.
- Zacznij już dziś bo ilość specjalistów na rynku jest skończona

itaudit




# Wnioski końcowe – czy NIS2 się opłaca?

🔴 Brak zgodności = wysokie ryzyko ataku i kar
🟡 Koszty wdrożenia NIS2 mogą być wysokie, ale da się je optymalizować
🟢 Dobra strategia = minimalizacja kosztów i ochrona przed cyberatakami

Koszt wdrożenia **NIS2 (10 mln zł)** jest niższy niż koszty potencjalnego ataku **(50 mln zł).**

(wyliczenia na podstawie roboczogodzin i kar które Państwo nałożyło by na podmiot – Incydent miał miejsce w Styczniu 2025 w Szczecinie)

**NIS2 daje możliwość uniknięcia kar i strat – lepiej inwestować w prewencję!**

**I być zgodnym z prawem i regulacjami w całej Unii Europejskiej ( brak zgodności może doprowadzić do utraty klientów)**

itaudit