Legacy Turn
Grupa LT Mastery

SERIA: LEGACYTURN

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) i NIS2 w Praktyce

Szablony

— kompletny przewodnik —

68 szablonów dla podmiotów kluczowych i ważnych

UoKSC Dz.U. 2026 poz. 252	**NIS2** Dyrektywa UE 2022/2555
Rozp. 2024/2690 Rozp. Wykonawcze KE (UE)	**ISO/IEC 27001:2022** Norma zarządzania bezpieczeństwem

Piotr Szymczyk

Ekspert cyberbezpieczeństwa · Audytor ISO/IEC 27001 · ICVC-SURE

Pobierz bezpłatnie — zeskanuj lub odwiedź

legacyturn.com/ltsklep

SERIA LEGACYTURN

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) i NIS2 w praktyce

Dokumentacja - Przewodnik po 68 szablonach dla podmiotów kluczowych i ważnych

Piotr Szymczyk

LegacyTurn · 2026

Bezpłatny e-book dostępny na legacyturn.com/ltsklep

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) i NIS2 w praktyce

Kompletny przewodnik po 68 szablonach NIS2/UoKSC dla podmiotów kluczowych i ważnych

Seria: LegacyTurn – Cyberbezpieczeństwo i Compliance

Wydanie: Pierwsze, 2026

Autor: Piotr Szymczyk

Ekspert cyberbezpieczeństwa, audytor, wykładowca, trener

E-mail: biuro@legacyturn.com · www.legacyturn.com

legacyturn.com/ltsklep - pełna biblioteka 68 szablonów NIS2/UoKSC

Dwupak: UoKSC i NIS2 w praktyce (Druk + E-book) - LegacyTurn Grupy LT Mastery – E-book „UoKSC i NIS2 w praktyce Praktyczny podręcznik implementacji Krajowego Systemu Cyberbezpieczeństwa, Frameworki, procedury, audyt dla zarządów, IT i compliance"

mailto:biuro@legacyturn.com - konsultacje i audyty wdrożeniowe

legacyturn.pl - Akademia Cyber LegacyTurn, szkolenia i społeczność

ISBN: 978-83-981562-2-6

> *Informacje zawarte w tej publikacji mają charakter ogólnoedukacyjny i informacyjny. Autor dołożył wszelkich starań, aby treści były jak najbardziej aktualne i zgodne ze stanem prawnym na dzień oddania do druku (2026 r.). Publikacja nie stanowi porady prawnej. W sprawach wymagających interpretacji prawnej skonsultuj się z licencjonowanym prawnikiem lub audytorem KSC.*

© LegacyTurn 2026. Wszelkie prawa zastrzeżone. Bezpłatna dystrybucja dozwolona wyłącznie w formie niezmienionej, z zachowaniem informacji o autorze i źródle.

Wstęp

Audytor przyjeżdża w czwartek

Jest środa rano, pierwszy dzień audytu w podmiocie kluczowym sektora dystrybucji energii. CISO jest spokojny. Przez ostatnie miesiące zrobili z zespołem tytaniczną pracę: wdrożony SIEM, EDR, bezwzględne MFA dla administratorów, backup offline według żelaznej reguły 3-2-1. Technicznie – forteca.

Audytor siada przy stole, otwiera laptopa i zadaje pierwsze pytanie: – *Proszę pokazać politykę bezpieczeństwa z podpisem prezesa i datą zatwierdzenia.*

W pokoju nagle zapada cisza.

Dokument istnieje. Od roku wisi na sharedrive, wszyscy pracownicy go znają. Ale prezes go nie podpisał. Nikt go o to nie poprosił, bo przecież wszyscy żyli wdrożeniami technicznymi. Jeśli coś nie jest udokumentowane i podpisane przez szefa, to dla audytora nie istnieje. W efekcie, mimo świetnie działających zabezpieczeń, organizacja formalnie nie spełniła wymogów. To zimny prysznic, który pokazuje, że w podmiotach kluczowych procedury i podpisy są tak samo ważne jak najlepsze wdrożenia techniczne.

> *Ta książka to przewodnik, który ma uchronić Cię przed podobnym scenariuszem. Pokazuje, jak domknąć wszystkie procesy. Od wdrożeń systemów po podpisy zarządu, tak aby Twoja praca obroniła się przed każdym, nawet najbardziej drobiazgowym audytorem.*

Dokumentacja NIS2 i UoKSC nie jest biurokracją dla biurokracji. To język, którym rozmawiasz z audytorem KSC, organem właściwym i, w razie incydentu, z sądem administracyjnym. Bez tego języka możesz mieć najlepszą infrastrukturę w sektorze i nadal przegrać kontrolę.

Biblioteka 68 szablonów którą opisuje ta książka to odpowiedź na jedno pytanie: co dokładnie musi istnieć w formie dokumentu, żeby Twój SZBI był kompletny i obronny: przed audytorem, przed organem, przed karą.

Nie wszystkie 68 dokumentów potrzebujesz od pierwszego dnia. Powiem Ci które są krytyczne, w jakiej kolejności je wdrażać. I od razu zaznaczam, to nie jest kolejna publikacja przepisująca ustawę. Tu znajdziesz to, co widzę na audytach: błędy, braki, skróty, które można wyeliminować dobrą dokumentacją i wdrożeniem technicznym.

Zaczynamy.

Dla kogo jest ten e-book?

- Dla CISO, który właśnie układa SZBI i szuka realnej mapy drogowej: co robić krok po kroku, w jakiej kolejności
- Dla Compliance Officera, który przygotowuje zgłoszenie z art. 46 (KSC) i chce wiedzieć, w które miejsca audytor uderzy na samym początku
- Dla Prezesa i Dyrektora Generalnego, którzy mają świadomość, że odpowiadają osobiście (i to finansowo, do wysokości 300% wynagrodzenia), więc chcą konkretu: co dokładnie muszą podpisać, żeby spać spokojnie
- Dla Audytora, który chce mieć czarno na białym wzorzec kompletnej dokumentacji, zanim wejdzie na kontrolę do podmiotu kluczowego

Sam e-book jest całkowicie **bezpłatny**. I nie mówimy tu o krótkiej broszurce reklamowej. Dostajesz do ręki konkretną, mięsistą wiedzę, która sama w sobie pomoże poukładać cały proces dokumentacji.

Jeśli po lekturze zechcesz zaoszczędzić czas i nie pisać wszystkiego od zera, to na **legacyturn.com/ltsklep** czeka pełna biblioteka **68 gotowych szablonów dokumentów**. To czyste narzędzie do pracy, gotowe do wdrożenia od zaraz.

Napisałem tę książkę i stworzyłem bibliotekę szablonów z jednego powodu: dobra dokumentacja SZBI/NIS2/UoKSC nie powinna być dostępna tylko dla organizacji, które stać na zewnętrznego konsultanta.

Prowadząc szkolenia, widzę że organizacje wiedzą co powinny zrobić. Rozumieją wymagania coraz lepiej. Mają ludzi, którzy chcą wdrożyć SZBI i być zgodnymi z ustawą o KSC. Ale często na etapie dokumentacji robi się dla nich ciężej, bo tworzenie jej od zera zajmuje miesiące i może kosztować nawet dziesiątki tysięcy złotych.

UoKSC objął setki polskich organizacji, które nigdy wcześniej nie miały do czynienia z formalnym systemem zarządzania bezpieczeństwem informacji. Wiele z nich ma deadline na rejestrację S46, 12 miesięcy na wdrożenie i budżet na bezpieczeństwo, który nie przewidywał tej pozycji. To jest rzeczywistość z którą zderzam się coraz częściej rozmawiając z CISO i compliance officerami po wejściu w życie ustawy.

Biblioteka 68 szablonów spełnia wymagania czterech aktów prawnych jednocześnie: Ustawy o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2026 poz. 252), Dyrektywy NIS2 (UE 2022/2555), Rozporządzenia Wykonawczego Komisji (UE) 2024/2690 oraz normy ISO/IEC 27001:2022. Każdy dokument ma przypisaną podstawę prawną i wskazanie co sprawdza audytor KSC. Żaden szablon nie istnieje bez powodu.

Architektura stworzona dla efektywności: Dlaczego akurat 68 szablonów?

Wdrożenie wymagań regulacyjnych w obszarze cyberbezpieczeństwa wiąże się z ryzykiem wpadnięcia w tzw. **pułapkę długu dokumentacyjnego**. Nadmiar ogólnych procedur i instrukcji często paraliżuje organizację, generując setki roboczogodzin potrzebnych na ich dostosowanie, a później ich utrzymanie.

Liczba 68 dokumentów w naszym pakiecie nie jest przypadkowa, i tworzy precyzyjnie zaprojektowany, zamknięty ekosystem stworzony z myślą o maksymalnej użyteczności i pełnym bezpieczeństwie prawnym Twojej organizacji oraz Zarządu.

- Optymalizacja i brak „martwej biurokracji”: Każdy wdrożony dokument to realne zobowiązanie dla firmy, z którego rozliczy Cię audytor. Nasz zestaw to wynik aptekarskiego zmapowania 10 obszarów Ustawy o KSC oraz 93 kontroli normy ISO/IEC 27001:2022. Otrzymujesz dokładnie te dokumenty, które są niezbędne do wykazania zgodności, bez obciążania zespołu zbędną administracją
- Pełna zgodność z polską specyfiką prawną (Seria KSC-): Nasz pakiet został stworzony ściśle pod kątem polskiej nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa. Zawiera unikalne, operacyjne szablony z prefiksem KSC- (m.in. Charakterystyka Usługi Kluczowej **KSC-CHU-001** czy Opis Zabezpieczeń Technicznych **KSC-OZT-001**), które wynikają wprost z art. 10 krajowej ustawy i stanowią kluczowy punkt każdej kontroli w Polsce
- Doświadczenie korporacyjne przekute w User Experience (UX): Po ponad 20 latach pracy w strukturach korporacyjnych doskonale wiem, jak uciążliwe i nieefektywne bywa ręczne zarządzanie setkami pojedynczych plików. Dlatego fundamentem naszego pakietu są dziś zaawansowane, interaktywne narzędzia w formacie Excel (w tym m.in. arkusz analizy ryzyka **R-ARC-001.xlsx**), które automatyzują aktywności, wyliczenia i przygotowują raporty dla Zarządu.

- Nadchodzi nowa era wdrożeń (Lokalne aplikacje webowe): Aby zapewnić jak najlepsze doświadczenia z pracy z dokumentami dla Ciebie i Twojego zespołu, w najbliższym czasie kluczowa część naszych narzędzi zostanie przeniesiona do formy lokalnych aplikacji webowych. Narzędzia te pobierzesz i uruchomisz bezpośrednio na swoim komputerze bądź wewnętrznym serwerze, co umożliwi płynną, wspólną pracę całego zespołu, gwarantując jednocześnie 100% bezpieczeństwa danych (żadne poufne informacje o Twojej infrastrukturze nie trafią do chmur zewnętrznych)
- Pakiet, który rośnie razem z rynkiem (Czegoś brakuje? Daj nam znać!): Przepisy i praktyki audytowe ewoluują. Choć 68 szablonów stanowi obecnie kompletny fundament zgodności, jednak każda organizacja ma swoją specyfikę. Jeśli podczas wdrożenia uznasz, że brakuje Ci jakiegoś konkretnego formularza lub procedury dopasowanej do Twojej branży – powiedz nam o tym. Nieustannie rozwijamy ten pakiet i chętnie stworzymy lub uzupełnimy brakujące elementy, aby dostarczyć Ci maksymalną wartość.

Wybierając ten pakiet, nie kupujesz „kartek do czytania", ani uniwersalnych wzorów skopiowanych z internetu. Inwestujesz w żywą, stale rozwijaną architekturę dokumentacyjno-narzędziową. Pozwala ona skrócić czas wdrażania wymogów dokumentacyjnych z kilku miesięcy do zaledwie 4–8 tygodni, łącząc rygorystyczne wymogi prawa z najwyższym komfortem codziennej pracy zespołowej.

Im więcej polskich organizacji ma porządną dokumentację SZBI, tym bezpieczniejsza polska infrastruktura krytyczna. To jest nasza misja – misja LegacyTurn.

> *Ważna informacja prawna: ta książka nie jest komentarzem prawnym ani oficjalną wykładnią przepisów. Jest podręcznikiem operacyjnym dla profesjonalistów, którzy muszą działać. Nie zastępuje indywidualnej porady prawnej ani dedykowanego audytu zgodności.*

1.0 Rozdział 1 – Mapa prawna, czyli jakie dokumenty powinieneś mieć i kiedy

Regulacje cybernetyczne UE eksplodowały. W ciągu kilku lat pojawiły się NIS2, nowelizacja UoKSC, Cyber Resilience Act, DORA, AI Act. Każda nakłada kolejne obowiązki, mówi nieco innym językiem i dotyczy nieco innych podmiotów.

Dobra wiadomość: dokumentacja NIS2 i UoKSC, którą budujesz pokrywa wymagania większości z tych aktów jednocześnie. Zarządzanie ryzykiem, obsługa incydentów, łańcuch dostaw: te tematy powtarzają się w każdej regulacji. Jedno wdrożenie, wiele efektów.

Zła wiadomość: musisz wiedzieć od czego zacząć i co jest prawnie wymagalne, a co tylko zalecane.

1.1 Art. 8 UoKSC: 10 obszarów, 68 dokumentów

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2026 poz. 252) nakłada na każdy Podmiot Kluczowy i Podmiot Ważny obowiązek wdrożenia środków bezpieczeństwa w 10 obszarach. Bez wyjątku. Bez różnicy między PK a PW: wymagania wdrożeniowe są identyczne dla obu. Różni je tylko model nadzoru i wysokość kar.

Każdy z tych 10 obszarów przekłada się na konkretne dokumenty. Nie na ogólne "polityki bezpieczeństwa", ale na konkretne: kto zatwierdził analizę ryzyka, kiedy ostatnio testowano backup, jakie klauzule są w umowach z dostawcami ICT.

Biblioteka 68 szablonów pokrywa wszystkie 10 obszarów — część z nich wielokrotnie. Nie dlatego, że lubię tworzyć dokumenty dla samego tworzenia. Ale dlatego, że audytor każdy obszar sprawdza inaczej i z innej perspektywy.

> **Ważne:** PK i PW mają identyczne wymagania wdrożeniowe. Klasyfikacja określa model nadzoru i wysokość kar, nie to co musisz wdrożyć. Organizacje, które myślą że status PW daje im taryfę ulgową przekonują się o tym dopiero przy pierwszym incydencie

1.2 ISO/IEC 27001:2022: 93 kontrole, wszystkie pokryte

Norma ISO/IEC 27001:2022 nie jest prawnie wymagana przez UoKSC. Ale audytor korzysta z jej struktury. Ministerstwo Cyfryzacji w swoim szablonie audytu wprost odwołuje się do wymagań ISO. Jeśli chcesz rozmawiać językiem audytora, powinieneś znać ISO.

Norma ma 93 kontrole bezpieczeństwa w Załączniku A. Podzielone na cztery kategorie: organizacyjne, personalne, fizyczne i technologiczne.

Wychodząc od bazowej analizy ISO/IEC 27001:2022, pierwsze 37 szablonów naszej biblioteki pokrywało 46% kontroli w pełni, a kolejne 33% w sposób częściowy. To jednak było za mało na rygorystyczne wymogi NIS2 oraz polskiej Ustawy o KSC.

Dlatego zrobiliśmy krok milowy. Rozbudowaliśmy architekturę do precyzyjnie zaprojektowanej listy 68 dokumentów, która stanowi dziś kompletny, zamknięty ekosystem zgodności prawnej i bezpieczeństwa Zarządu.

Czy ta liczba jest ostateczna? Przepisy i praktyki audytowe ewoluują, dlatego nasza biblioteka stale rośnie razem z rynkiem. Już teraz, analizując najnowsze niezgodności audytowe (jak choćby brak formalnego powiązania Incydentów z Zarządzaniem Zmianą), przygotowujemy kolejne dedykowane

szablony (np. procedurę **Z-PZM-002**), które będą sukcesywnie zasilać pakiet jako bezpłatne aktualizacje dla naszych klientów.” szablony (np. procedurę

> Biblioteka 68 szablonów adresuje wszystkie 93 kontrole ISO/IEC 27001:2022. Dwanaście dodatkowych dokumentów, pokrywa wymagania wprost z art. 10 UoKSC dotyczące dokumentacji: charakterystykę usługi kluczowej (**KSC-CHU-001**), ocenę stanu ochrony (**KSC-GAP-**001), opis zabezpieczeń technicznych (**KSC-OZT-001**) i dokumentację techniczną systemu (**KSC-DSI-001**). Do tego dochodzą formularze zgłoszeń do CSIRT (**KSC-FSC-001, KSCFSK-001**), oświadczenie zarządu (**KSC-OZK-001**) i formularz rejestracji S46 (**KSC-PKL-001**). Trzy z tych dokumentów dostępne są bezpłatnie, szczegóły w Rozdziale 3

1.3 Terminy których nie wolno przegapić

Zegar tyka. Piszę to w 2026 roku i mam poczucie że spora część polskich podmiotów kluczowych i ważnych nadal nie w pełni rozumie jak blisko jest deadline, czyli termin końcowy:

> **3 października 2026** : deadline rejestracji S46
>
> Każdy PK i PW który nie jest wpisany z urzędu, musi złożyć wniosek S46 do tego dnia. To nie jest termin na wdrożenie SZBI, to termin na rejestrację. Sprawdź najpierw wykaz-ksc.gov.pl, bo część podmiotów jest wpisywana automatycznie

> **24 miesiące od wpisu** : pierwszy audyt KSC dla Podmiotów Kluczowych
>
> Wpis z wniosku: zegar startuje w dniu złożenia wniosku w S46. Kto rejestruje się 3.10.2026, ma audyt do 3.10.2028.
>
> Wpis z urzędu: zegar startuje od daty decyzji organu. Część podmiotów już ma biegnący termin.
>
> Wdrożenie SZBI dla średniej organizacji: 7–8 miesięcy. Dla dużej z OT: 12–18 miesięcy.
>
> Organizacja, która wpisuje się 3.10.2026 i zaczyna następnego dnia, ma realnie 6–18 miesięcy na wdrożenie przed audytem.
>
> Faza dokumentacyjna bez szablonów: około 3–4 miesiące. Z biblioteką LegacyTurn: 4–6 tygodni. Oszczędność: 6–8 tygodni, czyli nawet połowa czasu dokumentacyjnego wraca z powrotem do wdrożenia technicznego.

> **3 kwietnia 2028** : pełna wymagalność kar finansowych
>
> Do 10 mln EUR lub 2% globalnego obrotu dla organizacji. Do 300% wynagrodzenia dla kierownika: osobista, niezależna od kary dla organizacji. Kary egzekwowane są po upływie 2 lat od wejścia w życie ustawy.

Wiem, że są organizacje które patrzą na termin kar i myślą: mamy czas do 2028. Nie mają. Audyt który ujawni braki w dokumentacji w 2027 roku nie jest bezbolesny. Organ może wydać decyzję nakazową, nałożyć środki naprawcze i monitorować wykonanie. Kary to ostateczność, ale kontrola i decyzje nakazowe działają już od 2026.

Dlatego zacznij już teraz.

1.4 Rozporządzenie WE 2024/2690: wymagania techniczne

Jest jeszcze jeden akt prawny który warto znać, bo pojawia się w wielu szablonach tej biblioteki: Rozporządzenie Wykonawcze Komisji (UE) 2024/2690. Obowiązuje bezpośrednio w całej UE. Bez implementacji krajowej.

Dotyczy konkretnych podmiotów: dostawców usług zarządzanych (MSP/MSSP), dostawców DNS, TLD, chmury, CDN i platform cyfrowych. Jeśli jesteś jednym z nich, to Twój akt prawny tak samo jak UoKSC.

Dla pozostałych podmiotów kluczowych i ważnych Rozporządzenie wyznacza techniczne wymagania dla wybranych środków bezpieczeństwa: zasady uwierzytelniania (pkt 11), zarządzanie ryzykiem łańcucha dostaw (pkt 5) i obsługa aktywów (pkt 2). W szablonach biblioteki odwołania do tego Rozporządzenia pojawiają się tam, gdzie przepis jest konkretny i egzekwowalny.

> *Rozporządzenie 2024/2690 używa sekcji (pkt), nie artykułów z podpunktami. Jeśli widzisz "Rozp. WE 2024/2690 pkt 11.3.2 lit. a", to prawidłowe cytowanie. "Art. 11 ust. 3 lit. a" takiego rozporządzenia po prostu nie ma*

1.5 Jak regulacje na siebie wpływają

Jedno wdrożenie może spełniać wymagania kilku regulacji jednocześnie. To nie jest zbieg okoliczności, to efekt celowego projektowania europejskiego prawa cybernetycznego.

Zarządzanie ryzykiem jest wymagane przez UoKSC, NIS2, DORA, CRA, RODO i AI Act jednocześnie. Procedura zarządzania incydentami spełnia jednocześnie art. 11 UoKSC i art. 33 RODO, wystarczy że jedna procedura ma dwa tory: zgłoszenie do CSIRT i zgłoszenie do UODO. Łańcuch dostaw ICT pojawia się w UoKSC, NIS2 i CRA.

Oznacza to jedno: zamiast budować osobne projekty dla każdej regulacji, zbuduj SZBI raz i pokaż jak spełnia wymagania różnych aktów. Biblioteka 68 szablonów jest zaprojektowana dokładnie w tym celu, każdy dokument ma w nagłówku podstawy prawne z kilku regulacji jednocześnie.

Wyjątek: DORA ma pierwszeństwo przed NIS2 w sektorze finansowym. Banki, ubezpieczyciele i fintech wdrażają wymagania DORA jako podstawowe, a tam gdzie DORA nie reguluje, stosują NIS2/UoKSC. To są osobne tory raportowania incydentów: KNF i CSIRT.

> **Podsumowanie rozdziału:** Masz trzy daty: 3 października 2026, 24 miesiące od wpisu, 3 kwietnia 2028. Pierwsza dotyczy rejestracji, druga pierwszego audytu, trzecia kar. Między pierwszą a trzecią jest czas na zbudowanie kompletnej dokumentacji. Nie jest go dużo.

Następny rozdział: jak jest zbudowana biblioteka 68 szablonów i dlaczego ma sens w tej właśnie formie.

Trzy kroki po zamknięciu tej książki

1. Wejdź na legacyturn.com/ltsklep i kup pełną **bibliotekę 68 szablonów** (**GRATIS e-book** „UoKSC i NIS2 w praktyce. Praktyczny podręcznik implementacji Krajowego Systemu Cyberbezpieczeństwa. Frameworki, procedury, audyt dla zarządów, IT i compliance) . Jeśli chcesz zacząć od trzech darmowych próbek, są dostępne do pobrania na stronie LegacyTurn **legacyturn.com/ltsklep,** a później w Akademii i uwaga dostępne są również na końcu tego e-book'a.
2. jeśli wypełnienie biblioteki we własnym zakresie to za dużo jak na zasoby które masz, umów konsultację. Jedna sesja robocza z osobą, która zna wymagania od środka często oszczędza kilka miesięcy błądzenia. Kontakt: **mailto:biuro@legacyturn.com**

Po trzecie: jeśli chcesz być na bieżąco z aktualizacjami prawa, praktyką audytową i nowymi szablonami, dołącz do Akademii LegacyTurn. Otwarcie platformy planowane na Lipiec 2026.

> **legacyturn.com/ltsklep -** pełna biblioteka 68 szablonów NIS2/UoKSC
>
> **mailto:biuro@legacyturn.com -** konsultacje i audyty wdrożeniowe
>
> **legacyturn.pl** - Akademia Cyber LegacyTurn, szkolenia i społeczność

Piotr Szymczyk

LegacyTurn · **mailto:biuro@legacyturn.com**

O autorze

Piotr Szymczyk to ekspert cyberbezpieczeństwa, audytor i trener z ponad 25-letnim doświadczeniem w GRC i bezpieczeństwie informacji. Magister Informatyki i Ekonometrii Uniwersytetu Łódzkiego. Certyfikowany Audytor ISO/IEC 27001, AgilePM Practitioner, absolwent EITCA Academy of Information Security i ITIL 4.

Twórca marki LegacyTurn, firmy szkoleniowo-konsultingowej specjalizującej się w cyberbezpieczeństwie dla biznesu. Autor książki „UoKSC i NIS2 w praktyce" (2026). Prowadzi szkolenia zamknięte i otwarte dla zarządów, CISO i compliance officerów w Polsce i UE.

Przez ostatnie lata pomagał organizacjom z sektorów energetyki, zdrowia, finansów i administracji publicznej przejść przez klasyfikację PK/PW, wdrożenie SZBI. Efekty tej pracy są w tej książce i w bibliotece 68 szablonów.

Kontakt: mailto:biuro@legacyturn.com · +48 600 390 516 · www.legacyturn.com

---

Inne tytuły serii Cyber LegacyTurn:

UoKSC i NIS2 w praktyce - praktyczny podręcznik implementacji Krajowego Systemu Cyberbezpieczeństwa (KSC). Klasyfikacja PK/PW, rejestracja S46, analiza ryzyka, SZBI, incydenty, łańcuch dostaw, audyt KSC. Dla zarządów, CISO, compliance i audytorów. Dostępna na Dwupak: UoKSC i NIS2 w praktyce (Druk + E-book) - LegacyTurn Grupy LT Mastery

NIS2 in Practice — angielska adaptacja podręcznika dla CISO, board members i compliance teams w UE i USA. A Complete Guide to NIS2, CRA, DORA, AI Act and GDPR. W przygotowaniu.

© LegacyTurn 2026 · Wszelkie prawa zastrzeżone

legacyturn.com/ltsklep · mailto:biuro@legacyturn.com