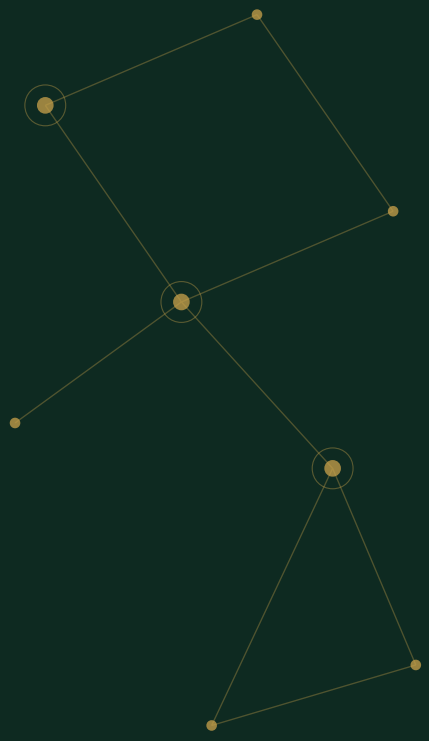
MK

Michał Krauze
EXECUTIVE ADVISORY



PRZEWODNIK DLA ZARZĄDÓW · 2026–2028

Odporna firma

NIS 2, DORA i AI Act bez paniki.
Trzy regulacje, jeden plan działania.

MICHAŁ KRAUZE

KRAUZEADVISORY.COM · STAN PRAWNY: 15 LIPCA 2026

SPIS TREŚCI

Co znajdziesz w środku

2.5. Czego oczekuje kontrola: artefakty i szablony

Lista dziesięciu środków brzmi abstrakcyjnie, dopóki nie przełożysz jej na dokumenty i dowody, które trzeba fizycznie pokazać podczas audytu lub kontroli. Poniższa mapa robi dokładnie to: dla każdego wymagania pokazuje, czego realnie oczekuje kontrolujący, jakie artefakty to potwierdzają i od jakiego szablonu zacząć. Zasada jest brutalnie prosta: **czego nie ma na piśmie, tego z punktu widzenia kontroli nie ma wcale**.

	Czego oczekuje kontrola	Artefakty (dowody)	Proponowany szablon startowy
Analiza ryzyka i polityki bezpieczeństwa	Udokumentowana metodyka, cykliczność (min. raz w roku i po istotnej zmianie), decyzje wynikające z ryzyka	Polityka bezpieczeństwa informacji; metodyka analizy ryzyka; rejestr ryzyk; plan postępowania z ryzykiem zatwierdzony przez zarząd	Rejestr ryzyk (arkusz: aktywo, zagrożenie, skutek, prawdopodobieństwo, właściciel, decyzja)
Obsługa incydentów	Zdolność wykrycia, klasyfikacji i eskalacji, nie tylko procedura	Procedura zarządzania incydentami; rejestr incydentów; playbooki dla typowych scenariuszy; raporty z obsłużonych zdarzeń	Playbook incydentu (ransomware / wyciek danych) + rejestr incydentów
Ciągłość działania	Plany, które ktoś faktycznie przetestował, z datą i podpisem	Plan ciągłości działania (BCP) i odtworzeniowy (DRP); polityka kopii zapasowych; harmonogram i protokoły testów odtworzenia	Protokół testu odtworzenia (co testowano, wynik, czas, wnioski)
Bezpieczeństwo łańcucha dostaw	Wiedza, którzy dostawcy są krytyczni i co jest w umowach	Polityka bezpieczeństwa dostawców; rejestr umów ICT; klauzule bezpieczeństwa i audytu; oceny	Rejestr umów ICT (dostawca, usługa, krytyczność, klauzule, data przeglądu, strategia wyjścia)

SZABLONY Z TEJ TABELI · GOTOWY PAKIET WDROŻENIOWY

Wszystkie dokumenty z kolumny "proponowany szablon" istnieją jako gotowy do wypełnienia pakiet: 19 szablonów (7 rejestrów w Excelu, m.in. rejestr ryzyk z automatycznym poziomem i rejestr incydentów pod terminy 24h/72h, oraz 12 dokumentów w Wordzie: polityki, playbook incydentu, plan ciągłości działania, protokoły) i trzy elementy premium: deck na posiedzenie zarządu z notatkami prelegenta, roadmapa wdrożenia na 12 miesięcy i kit corocznego szkolenia zarządu.

Masz wersję premium? Pakiet jest już w Twoich plikach do pobrania. **Kupiłeś samego ebooka?** Pakiet zamówisz osobno na **krauzeadvisory.com**.

2.6. Masz ISO 27001? Co certyfikat załatwia, a czego nie

Najczęstsza reakcja organizacji z wdrożonym ISO 27001 brzmi: "przecież mamy certyfikat". I to jest w dużej mierze dobra wiadomość: norma pokrywa większość merytoryki art. 21, a dokumentacja SZBI zbudowana pod ISO stanowi 70–80% drogi. Ale ustawa ma wymogi, których w normie nie ma, i to właśnie o nie potyka się firma pewna swojego certyfikatu. Mapa poniżej pokazuje, gdzie jesteś z ISO, a co musisz dołożyć.

Wymaganie art. 21 / ustawy KSC	Gdzie w ISO/IEC 27001:2022	Status z ISO
Analiza ryzyka i polityki bezpieczeństwa	kl. 6.1.2, 8.2; zał. A.5.1	pokryte
Obsługa incydentów	zał. A.5.24–A.5.28	częściowo
Ciągłość działania i kopie zapasowe	zał. A.5.29–A.5.30, A.8.13–A.8.14	pokryte
Bezpieczeństwo łańcucha dostaw	zał. A.5.19–A.5.23	częściowo
Rozwój, utrzymanie, podatności	zał. A.8.8, A.8.25–A.8.31	pokryte
Ocena skuteczności zabezpieczeń	kl. 9 (monitorowanie, audyt wewnętrzny, przegląd zarządzania)	pokryte
Higiena i szkolenia	zał. A.6.3	częściowo
Kryptografia	zał. A.8.24	pokryte
	zał. A.5.9–A.5.18, A.6.1–A.6.5, A.8.1–A.8.5	pokryte

4.1. Czym jest i jak myśli

Rozporządzenie (UE) 2024/1689 weszło w życie 1 sierpnia 2024 roku, z obowiązkami rozłożonymi etapami. Podobnie jak DORA obowiązuje bezpośrednio w całej UE. Najważniejsze, co trzeba zrozumieć: AI Act nie reguluje "sztucznej inteligencji" jako technologii. Reguluje **konkretne zastosowania według poziomu ryzyka**.

Rys. 4.1. Piramida ryzyka AI Act: im wyżej, tym mniej zastosowań i tym cięższe obowiązki.

- **Ryzyko niedopuszczalne, czyli praktyki zakazane** (od 2 lutego 2025): scoring społeczny, manipulacyjne techniki podprogowe, masowe scrapowanie wizerunków do baz rozpoznawania twarzy.
- **Wysokie ryzyko**: AI w rekrutacji i decyzjach kadrowych, scoringu kredytowym, edukacji, infrastrukturze krytycznej (Załącznik III) oraz AI wbudowane w produkty regulowane, jak wyroby medyczne czy maszyny (Załącznik I). Tu pełny pakiet obowiązków: system zarządzania jakością, dokumentacja techniczna, nadzór człowieka, ocena zgodności, rejestracja w bazie UE.
- **Ograniczone ryzyko**: obowiązki przejrzystości. Użytkownik musi wiedzieć, że rozmawia z AI; treści generowane przez AI i deepfake'i muszą być oznaczane.
- **Ryzyko minimalne**: brak dodatkowych obowiązków. To większość zastosowań AI w firmach.

Osobny reżim dotyczy **modeli AI ogólnego przeznaczenia (GPAI)**, czyli dużych modeli w rodzaju GPT czy Claude. Obowiązki ich dostawców (dokumentacja, polityka praw autorskich, dla największych modeli ocena ryzyk systemowych) obowiązują od 2 sierpnia 2025.

4.2. Uwaga: terminy zmieniły się w czerwcu 2026

To najbardziej aktualna część tego ebooka, więc czytaj uważnie, bo w internecie wciąż krąży mnóstwo nieaktualnych dat. W czerwcu 2026 UE przyjęła tak zwany **Digital Omnibus on AI**, pakiet zmian do AI Act.

4. **Traktowanie odroczenia AI Act jako odwołania.** Przesunięto terminy wysokiego ryzyka, ale przejrzystość wchodzi w sierpniu 2026, a zakazy już obowiązują.
5. **Kupowanie narzędzi przed zdefiniowaniem procesu.** SIEM bez ludzi i procedur to bardzo drogi generator alertów, których nikt nie czyta.

6.6. Ile to kosztuje: widełki rynkowe

Każdy plan wdrożenia prędzej czy później trafia na pytanie o budżet. Odpowiedź zależy przede wszystkim od punktu startu organizacji: firma z żywym ISO 27001 i wynikiem 16/20 w checkliście samooceny wyda ułamek tego, co firma zaczynająca od zera. Zebrane poniżej widełki pochodzą z publikowanych cenników i analiz rynkowych (wartości netto, stan na lipiec 2026). Nie zastąpią indywidualnej wyceny, ale pozwalają zbudować pierwszy realny budżet i ocenić oferty dostawców.

	Mała firma (50–100 osób)	Średnia (100–250 osób)	Duża / podmiot kluczowy (250+)
Analiza luk i dokumentacja SZBI (jednorazowo)	15–40 tys. zł	30–80 tys. zł	60–150 tys. zł
Środki techniczne: MFA, EDR, kopie z izolacją, segmentacja (pierwszy rok)	20–60 tys. zł	50–150 tys. zł	150–500 tys. zł
Szkolenia i testy phishingowe (rocznie; szkolenie zarządu na rynku: 1–1,8 tys. zł/os.)	5–15 tys. zł	10–30 tys. zł	20–60 tys. zł
Monitoring / SOC zewnętrzny (miesięcznie)	2–8 tys. zł	8–25 tys. zł	20–50+ tys. zł
vCISO, jeśli brak własnego lidera bezpieczeństwa (miesięcznie, opcjonalnie)	4–8 tys. zł	8–15 tys. zł	15–25 tys. zł
Audyt zewnętrzny (dla kluczowych: pierwszy do kwietnia 2028)	15–40 tys. zł	30–80 tys. zł	50–150 tys. zł
Rząd wielkości: pierwszy rok	**60–120 tys. zł**	**80–180 tys. zł**	**250–600+ tys. zł**
Utrzymanie: kolejne lata	**30–60 tys. zł/ rok**	**50–100 tys. zł/rok**	**150–400+ tys. zł/rok**

Trzy komentarze do tych liczb, ważniejsze niż same liczby.

Po pierwsze: najdroższa pozycja nie jest w tabeli. Firmy najwięcej przepłacają nie na żadnej z powyższych pozycji, tylko na kolejności: kupują narzędzia przed zdefiniowaniem procesów (SIEM bez ludzi to generator alertów, których nikt nie czyta), biorą "pakiet pod NIS 2" od pierwszego vendora bez własnej

NARZĘDZIE

Checklista samooceny: gdzie jest Twoja firma

Dwadzieścia pytań, odpowiedzi wyłącznie "tak" albo "nie". "Tak" tylko wtedy, gdy istnieje dokument lub dowód. Deklaracje się nie liczą. Za każde "tak" jeden punkt.

Nr	Pytanie	Tak/ Nie
1	Mamy formalną, podpisaną decyzję, czy i w jakiej kategorii podlegamy pod ustawę KSC	
2	Jesteśmy zarejestrowani w wykazie (S46) albo mamy udokumentowaną decyzję, że nie podlegamy	
3	Jedna osoba (nie komitet) prowadzi program odporności z mandatem i budżetem od zarządu	
4	Mamy aktualny (młodszy niż 12 miesięcy) rejestr ryzyk zatwierdzony przez zarząd	
5	Mamy rejestr aktywów obejmujący systemy, dane i usługi zewnętrzne	
6	Mamy politykę bezpieczeństwa informacji zatwierdzoną przez zarząd	
7	Wiemy, kto i jak zgłasza poważny incydent do CSIRT, i przetestowaliśmy to ćwiczeniem	
8	Prowadzimy rejestr incydentów z czasami wykrycia i zgłoszenia	
9	Zrobiliśmy w ostatnich 6 miesiącach udany test odtworzenia kopii zapasowej, z protokołem	
10	Kopie zapasowe są odizolowane od domeny produkcyjnej (ransomware ich nie zaszyfruje)	
11	Mamy rejestr umów ICT z oceną krytyczności dostawców	
12	Umowy z krytycznymi dostawcami mają klauzule bezpieczeństwa, audytu i wyjścia	
13	MFA obejmuje 100% dostępu zdalnego i kont uprzywilejowanych, a wyjątki są w rejestrze z terminem	
14	Krytyczne podatności łatamy w zdefiniowanym SLA i umiemy to wykazać raportem	
15	Przegląd uprawnień odbył się w ostatnim kwartale, z protokołem	
16	Odbyło się w ostatnich 12 miesiącach szkolenie zarządu z cyberbezpieczeństwa, z dokumentem	
17	Prowadzimy cykliczne szkolenia i testy phishingowe dla wszystkich pracowników	

TO BYŁ PODGLĄD

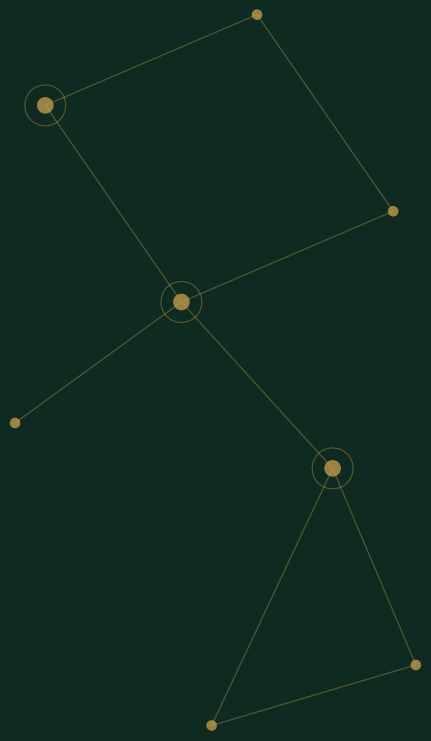
Pełne wydanie: 40 stron

6 rozdziałów · mapa artefaktów kontroli · mapowanie ISO 27001 · plan 90 dni
widełki kosztów · checklista 20 pytań · słownik 42 haseł

Ebook i pakiet wdrożeniowy: ***krauzeadvisory.com***
Bezpłatny fragment (cały rozdział 1) do pobrania na stronie.

MK

Michał Krauze
EXECUTIVE ADVISORY



A BOARDROOM GUIDE · 2026–2028

The Resilient Company

NIS 2, DORA and the AI Act without panic. Poland's new rules, one action plan.

MICHAŁ KRAUZE

KRAUZEADVISORY.COM · LEGAL STATUS: 15 JULY 2026

CONTENTS

What is inside

2.5. What an inspection expects: artefacts and templates

The list of ten measures sounds abstract until you translate it into the documents and evidence you will physically have to produce during an audit or inspection. The map below does exactly that: for each requirement it shows what the inspector realistically expects, which artefacts prove it, and which template to start from. The rule is brutally simple: **from an inspection's point of view, whatever is not in writing does not exist**.

	What the inspection expects	Artefacts (evidence)	Suggested starter template
Risk analysis and security policies	A documented methodology, a regular cycle (at least yearly and after material change), decisions driven by risk	Information security policy; risk methodology; risk register; risk treatment plan approved by the board	Risk register (sheet: asset, threat, impact, likelihood, owner, decision)
Incident handling	The ability to detect, classify and escalate, not just a procedure	Incident management procedure; incident register; playbooks for typical scenarios; reports from handled events	Incident playbook (ransomware / data leak) + incident register
Business continuity	Plans that someone has actually tested, with a date and signature	Business continuity (BCP) and recovery (DRP) plans; backup policy; restore-test schedule and protocols	Restore test protocol (what was tested, result, time, conclusions)
Supply chain security	Knowing which suppliers are critical and what is in the contracts	Supplier security policy; ICT contract register; security and audit clauses; supplier criticality assessments	ICT contract register (supplier, service, criticality, clauses, review date, exit strategy)
	A patching process with deadlines tied to criticality	Vulnerability management policy;	

	What the inspection expects	Artefacts (evidence)	Suggested starter template
	Evidence of management engagement	management declarations; documentation of the annual board training; management review minutes	Management review minutes (agenda, decisions, signatures)

THE MINIMUM SET · 15 DOCUMENTS EVERY INSPECTION STARTS FROM

Information security policy · risk register · asset register · incident management procedure with register · business continuity plan with test protocols · backup policy · ICT contract register · supplier security policy · vulnerability management procedure · access control policy · cryptographic policy · annual training plan with registers · CSIRT reporting procedure · management review minutes · board training documentation.

Two practical caveats. First, the final scope of documentation follows from your organisation's risk analysis, so treat this map as a starting point, not a closed list. Second, do not write these documents "for the inspection". A document that does not describe the actual process is worse during an inspection than no document at all, because it proves the system exists only on paper.

TEMPLATES FROM THIS TABLE · A READY-MADE IMPLEMENTATION PACK

Every document in the "suggested starter template" column exists as a fill-in-ready pack: 19 templates (7 Excel registers, including a risk register with automatic scoring and an incident register built around the 24h/72h deadlines, and 12 Word documents: policies, an incident playbook, a business continuity plan, protocols) plus three premium elements: a ready board presentation with speaker notes, a 12-month implementation roadmap, and a complete annual board-training kit.

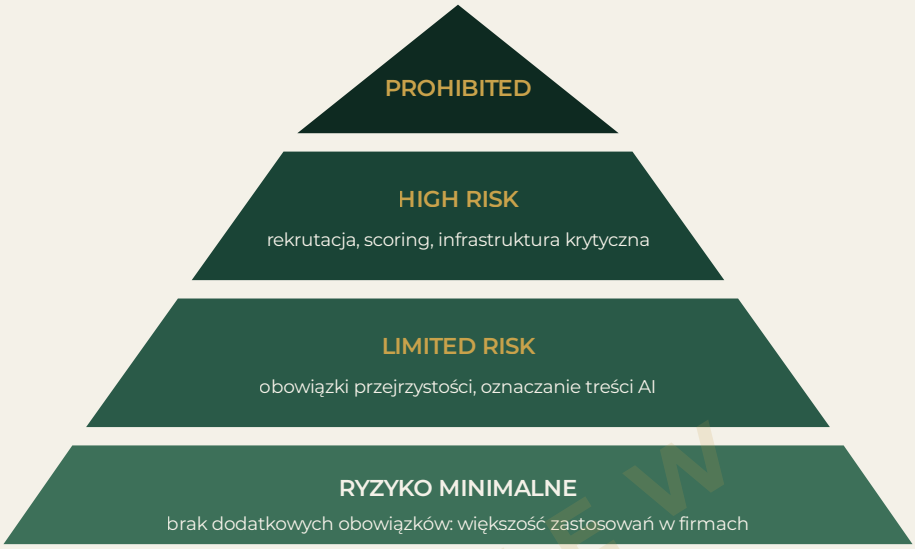
Bought the premium edition? The pack is already in your downloads. **Bought the ebook alone?** The pack is available separately at **krauzeadvisory.com**.

2.6. Already ISO 27001 certified? What the certificate covers, and what it does not

The most common reaction from organisations with ISO 27001 in place is: "but we are certified". And that is largely good news: the standard covers most of the substance of Article 21, and ISMS documentation built for ISO takes you 70–80% of the way. But the Polish act contains requirements the standard does

4.1. What the AI Act is

Regulation (EU) 2024/1689 is the world's first attempt to regulate artificial intelligence comprehensively. Like DORA, it applies directly across the EU. Its architecture is a risk pyramid: the higher the risk a given use of AI carries for people, the heavier the obligations.



The bans (e.g. social scoring, manipulative techniques exploiting vulnerabilities) have applied since February 2025. General-purpose AI (GPAI) model obligations have applied since August 2025. For a typical company, the two layers that matter are high risk and transparency.

4.2. Deadlines after the June 2026 changes

In June 2026, the EU adopted the Digital Omnibus on AI (European Parliament: 16 June, Council: 29 June 2026), a simplification package that shifted parts of the calendar. The current schedule:

Obligation	Deadline
Bans on prohibited practices; AI literacy duty	in force since 2 Feb 2025
GPAI model obligations	in force since 2 Aug 2025
Article 50 transparency duties (chatbot disclosure, deepfake labelling)	**2 August 2026 (unchanged)**
Machine-readable marking, Art. 50(2), for systems already on the market before 2 Aug 2026	2 December 2026 (grace period)
Ban on non-consensual intimate imagery generation	2 December 2026
High-risk systems, Annex III (standalone)	2 December 2027 (was: Aug 2026)
High-risk systems, Annex I (embedded in regulated products)	2 August 2028

— Management reviews with minutes: in all three regimes the management body answers, so it must be able to show it runs the topic. In an inspection, the winner is not who did the work but who holds the evidence

— Preparation for AI Act high-risk duties (December 2027), if they apply

6.5. The five most common mistakes

1. **"We have ISO 27001, so we are compliant."** ISO is an excellent skeleton, but the Polish act has requirements outside the standard (the register, documented board training, reporting deadlines). The certificate is the starting point, not the finish line.
2. **Waiting for "guidelines".** Ministries publish interpretive material, but the deadlines run regardless of how informed you feel.
3. **Delegating downwards without a mandate.** If the programme is run by an IT specialist without budget or access to the board, it is not a programme, it is an alibi.
4. **Treating the AI Act deferral as a cancellation.** High-risk deadlines moved; transparency lands in August 2026 and the bans already apply.
5. **Buying tools before defining the process.** A SIEM without people and procedures is a very expensive generator of alerts nobody reads.

6.6. What it costs: market ranges

Every implementation plan sooner or later runs into the budget question. The answer depends above all on the organisation's starting point: a company with a living ISO 27001 and a 16/20 checklist score will spend a fraction of what a company starting from zero will. The ranges below come from published price lists and market analyses (net values, as at July 2026). They will not replace an individual quote, but they let you build a first realistic budget and evaluate vendor offers. Amounts are in Polish złoty (PLN; roughly 4.3 PLN per EUR).

	Small company (50–100 staff)	Medium (100–250)	Large / essential entity (250+)
Gap analysis and ISMS documentation (one-off)	PLN 15–40k	PLN 30–80k	PLN 60–150k
Technical measures: MFA, EDR, isolated backups, segmentation (first year)	PLN 20–60k	PLN 50–150k	PLN 150–500k
Training and phishing tests (yearly; market rate for board training: PLN 1–1.8k/person)	PLN 5–15k	PLN 10–30k	PLN 20–60k
External monitoring / SOC (monthly)	PLN 2–8k	PLN 8–25k	PLN 20–50k+

THIS WAS A PREVIEW

Full edition: 37 pages

6 chapters · inspection artefact map · ISO 27001 mapping · 90-day plan
cost ranges · 20-question checklist · 42-term glossary

Ebook and implementation pack: ***krauzeadvisory.com***
Free sample (full chapter one) available on the site.