

Szanowni Państwo,

w imieniu wydawcy miesięcznika "IT Professional" oraz p. Artura Cieślika zapraszam na:

## SZKOLENIE ONLINE

### **„Nowa ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) - obowiązki, samoocena, projekt wdrożenia”**

**21 maja 2026 roku (czwartek) na profesjonalnej platformie do SZKOLEŃ ONLINE**

*\*Artur Cieślik - certyfikowany audytor wiodący normy ISO/IEC 27001, specjalizuje się w audycie bezpieczeństwa informacji i wdrażaniu Systemów Zarządzania Bezpieczeństwem Informacji; praktyk, inżynier, specjalizuje się w zabezpieczeniach systemów i aplikacji oraz w projektowaniu wielopoziomowych rozwiązań bezpieczeństwa; redaktor naczelny miesięcznika „IT Professional”; prelegent na licznych konferencjach; członek rady programowej kwartalnika „ABI Expert”; współtwórca i wykładowca studiów podyplomowych w zakresie bezpieczeństwa informacji i systemów informatycznych.*

**Nowa ustawa o Krajowym Systemie Cyberbezpieczeństwa istotnie zmienia otoczenie regulacyjne organizacji, wprowadzając rozbudowane obowiązki techniczne i organizacyjne oraz nowe role po stronie kierownictwa.** Przepisy są złożone, silnie powiązane z dyrektywą NIS2 i aktami wykonawczymi UE, a ich interpretacja w praktyce rodzi liczne wątpliwości. Błędy we wdrożeniu mogą skutkować odpowiedzialnością prawną, sankcjami administracyjnymi oraz realnym wzrostem ryzyka operacyjnego i reputacyjnego.

**Szkolenie obejmuje** omówienie podstaw prawnych i terminologii nowej ustawy o KSC, identyfikację podmiotów objętych regulacją oraz szczegółowe wymagania w zakresie zarządzania ryzykiem, incydentami i ciągłością działania. **Przedstawione zostanie** powiązanie przepisów z wytycznymi ENISA, rozporządzeniem wykonawczym 2024/2690 oraz normami ISO/IEC 27001 i ISO 22301.

**Integralną częścią programu jest** samoocena zgodności, analiza luk, przygotowanie projektu wdrożenia oraz **warsztat modelowania ryzyka** i ustalania wymagań minimalnych.

**Warsztaty przygotowane zostały dla** administratorów systemów, inspektorów ochrony danych, oficerów bezpieczeństwa oraz kadry kierowniczej.

Szkolenie odbędzie się 21 maja 2026 roku (czwartek) na profesjonalnej platformie do SZKOLEŃ ONLINE.

**Warunkiem uczestnictwa jest dokonanie wpłaty** na konto organizatora **oraz przesłanie zgłoszenia** na e-mail: szkolenia@itprofessional.pl lub numer faksu: 71 798 48 48 albo wypełnienie formularza na stronie [www: szkolenia.itprofessional.pl/t/KSCN](http://www.szkolenia.itprofessional.pl/t/KSCN)

W razie wątpliwości pozostajemy do Państwa dyspozycji pod numerem telefonu: 71 798 48 40.

Z poważaniem,

**Arkadiusz Karasek**

wydawca miesięcznika „IT Professional”

- **Szkolenie w czasie rzeczywistym**  
- nie jest to uprzednio nagrany materiał
- **6 godzin wraz z przerwą**  
- rozpoczynamy o godz. 9.00
- **Możliwość zadawania pytań**  
i dyskusji z innymi uczestnikami
- **Grupa do 25 osób** - każdy będzie miał czas na zadawanie pytań
- **Niższa cena** - w porównaniu do szkolenia stacjonarnego
- **Wydrukowany certyfikat**  
- wyślemy pocztą
- **Dostępne na komputerze, tablecie i smartfonie** - z dowolnego miejsca

Pełny kalendarz naszych szkoleń  
i konferencji na stronie [www:  
szkolenia.itprofessional.pl](http://www.szkolenia.itprofessional.pl)

**HARMONOGRAM SZKOLENIA ONLINE****„Nowa ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) - obowiązki, samoocena, projekt wdrożenia”**

21 maja 2026 roku (czwartek), godz. 9.00-15.00 na profesjonalnej platformie do SZKOLEŃ ONLINE

1. **Podstawy prawne i terminologia:**
  - a. dyrektywa NIS2, projekt UoKSC (UC32), powiązane akty;
  - b. normy związane z nową UoKSC;
  - c. przegląd pojęć: podmiot kluczowy (PK), podmiot ważny (PW), systemy, incydenty, ryzyko, łańcuch dostaw;
  - d. terminy dostosowania.
2. **Wymagania projektu UoKSC - co wdrożyć:**
  - a. zakres podmiotowy (kto podlega);
  - b. podmioty kluczowa i ważne, wyjątkowe kategorie, zależność od wielkości;
  - c. zarządzanie ryzykiem w cyberbezpieczeństwie;
  - d. zapobieganie, wykrywanie i reagowanie na incydenty;
  - e. utrzymania ciągłości działania i zarządzania kryzysowego;
  - f. bezpieczeństwo łańcucha dostaw;
  - g. szkolenia w zakresie cyberbezpieczeństwa;
  - h. bezpieczeństwo sieci i systemów informacyjnych;
  - i. polityki zarządzania i zgłaszania podatności;
  - j. bezpieczeństwo zasobów ludzkich, zarządzanie dostęпами i aktywami;
  - k. uwierzytelnianie wieloskładnikowe oraz ciągłe;
  - l. zabezpieczanie połączeń;
  - m. stosowanie kryptografii i szyfrowania.
3. **Od wytycznych Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i IR do praktyki wdrożenia:**
  - a. powiązanie wymagań projektu UoKSC z dobrymi praktykami ENISA;
  - b. odniesienie do rozporządzenia wykonawczego 2024/2690 - wymogi i oczekiwane zabezpieczenia na poziomie procesów i środków zarządzania ryzykiem;
  - c. mapowanie wymagań nowej UoKSC do ISO/IEC 27001 oraz ISO 22301.
4. **Samoocena (audyt 0) i plan działań:**
  - a. szablon samooceny zgodności z projektem UoKSC;
  - b. mapowanie wymagań art. 8-8h (środki zarządzania ryzykiem, polityki, szkolenia kierownictwa) na kontrolki i dowody;
  - c. lista braków (gap analysis) i priorytetyzacja;
  - d. projekt wdrożenia i wskaźniki KPI/KRI/KCI.
5. **Warsztat: model ryzyka i ustalanie wymagań minimalnych:**
  - a. zasady prowadzenia szacowania ryzyka;
  - b. stosowanie atrybutów cyberbezpieczeństwa;
  - c. przykłady ryzyk i action planów.
6. **Certyfikacja cyberbezpieczeństwa - informacje podstawowe:**
  - a. ramy prawne certyfikacji - rozporządzenie (UE) 2019/881 (Cybersecurity Act) oraz ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa;
  - b. rodzaje certyfikacji i poziomy zapewnienia (basic, substantial, high).
7. **Odpowiedzi na pytania uczestników szkolenia.**

**Jak wygląda szkolenie online?**

1. **Zgłoszenia dokonujesz** wysyłając wypełnioną kartę zgłoszeniową na adres: [szkolenia@itprofessional.pl](mailto:szkolenia@itprofessional.pl), lub numer faksu: **71 798 48 48** lub poprzez formularz na stronie [www: szkolenia.itprofessional.pl/t/KSCN](http://www.szkolenia.itprofessional.pl/t/KSCN)
2. Na 2 dni przed szkoleniem na wskazane w zgłoszeniu adresy e-mail prześlemy unikatowe linki do platformy.
3. W dniu szkolenia logujesz się do platformy z dowolnego miejsca na dowolnym urządzeniu (komputer, tablet lub smartfon).
4. W trakcie szkolenia widać ekran prowadzącego oraz jego samego.
5. Możesz zadawać pytania trenerowi przez mikrofon lub wbudowany czat.
6. Materiały w formacie PDF będą do pobrania w trakcie szkolenia, a wydrukowany certyfikat otrzymasz pocztą.
7. Po zakończeniu szkolenia, nie ma możliwości jego ponownego odtworzenia.

**Co jest potrzebne od strony technicznej?**

- **Komputer z przeglądarką internetową** (Google Chrome, Mozilla Firefox, Safari, Microsoft Edge, Opera) **lub tablet lub telefon z bezpłatną aplikacją** do pobrania z Apple App Store lub Google Play Store.
- Można, ale nie trzeba używać podczas szkolenia wbudowanej kamery lub kamery internetowej, mikrofonu, zestawu słuchawkowego lub podłączonych głośników, ale nie powinny być one jednocześnie używane przez żadną inną aplikację.

## KARTA ZGŁOSZENIA NA SZKOLENIE ONLINE

### **„Nowa ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) - obowiązki, samoocena, projekt wdrożenia”**

**Prowadzenie: Artur Cieślík**

**21 maja 2026 roku (czwartek), godz. 9.00-15.00 na profesjonalnej platformie do SZKOLEŃ ONLINE**

Wypełnioną kartę prosimy przysyłać na numer faksu: **71 798 48 48** lub e-mail: [szkolenia@itprofessional.pl](mailto:szkolenia@itprofessional.pl)  
Zgłoszenia można także dokonać na stronie [www: szkolenia.itprofessional.pl/t/KSCN](http://www.szkolenia.itprofessional.pl/t/KSCN)

<b>1.</b>	Imię i nazwisko	Stanowisko	
	Telefon	E-mail (na który wyślemy unikatowy kod dostępu do platformy)	Kwota
<b>2.</b>	Imię i nazwisko	Stanowisko	
	Telefon	E-mail (na który wyślemy unikatowy kod dostępu do platformy)	Kwota
<b>RAZEM</b>			Suma kwot

**Koszt uczestnictwa 1 osoby w szkoleniu online wynosi 690 zł i obejmuje koszt materiałów w formie elektronicznej oraz wydrukowany certyfikat** przesyłany pocztą po szkoleniu. Przy zgłoszeniach na szkolenie nadesłanych po dniu 18 maja 2026 roku koszt uczestnictwa jednej osoby wynosi 790 zł. **Liczba miejsc ograniczona jest do 25.**

**Do podanych cen nie doliczamy podatku VAT po podpisaniu poniższego oświadczenia o finansowaniu ze środków publicznych.** W przeciwnym razie doliczamy podatek VAT w wysokości 23%.

**Oświadczam, że szkolenie korzysta ze zwolnienia z VAT, ponieważ stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego i jest finansowane w całości ze środków publicznych** zgodnie z art. 43 ust. 1 pkt 29c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (z późn. zm.).

\_\_\_\_\_  
Data, pieczętka, podpis

<b>DANE DO FAKTURY:</b>	Płatności prosimy realizować: <b>PRESSCOM Sp. z o.o., ul. Krakowska 29, 50-424 Wrocław</b> <b>Santander Bank Polska: 96 1090 1522 0000 0001 0162 2418</b> z tytułem płatności: <b>20260521KSCN</b>		
<b>DANE ODBIORCY:</b>	Nazwa		
	Ulica	Kod	Miejscowość
	NIP	IDWew / nr zamówienia	E-mail do księgowości
<b>DANE NABYWCY:</b>	Nazwa		NIP
	Ulica	Kod	Miejscowość

Przesłanie karty zgłoszenia stanowi prawnie wiążące zobowiązanie do uczestnictwa w szkoleniu na warunkach w niej określonych. Rezygnacji z udziału w szkoleniu można dokonać wyłącznie w formie pisemnej (e-mail, fax, poczta), najpóźniej 7 dni roboczych przed szkoleniem. W przypadku otrzymania rezygnacji przez organizatora później niż na 7 dni roboczych przed dniem szkolenia lub niezalogowania się uczestnika do platformy i tym samym niewzięcia udziału w szkoleniu, zgłaszający zostanie obciążony pełnymi kosztami uczestnictwa, wynikającymi z przesłanej karty zgłoszenia, na podstawie wystawionej faktury VAT. Niedokonanie wpłaty nie jest jednoznaczne z rezygnacją z udziału w szkoleniu.

Przesłanie zgłoszenia i podanie danych osobowych jest dobrowolne. Niepodanie wymaganych danych uniemożliwi realizację umowy/zamówienia. Informujemy, że Państwa dane osobowe będą przetwarzane w celach marketingu produktów i usług własnych Presscom Sp. z o.o. Administratorem danych osobowych będzie Presscom Sp. z o.o. z siedzibą we Wrocławiu, numer KRS 0000173413. Dane osobowe nie będą przekazywane podmiotom trzecim bez prawidłowej podstawy prawnej. W szczególności mają Państwo prawo do sprzeciwu wobec przetwarzania w celach marketingowych, a także żądania od Presscom Sp. z o.o. dostępu do swoich danych osobowych oraz ich sprostowania lub usunięcia. W sprawach z zakresu ochrony danych osobowych możliwy jest kontakt z [do@presscom.pl](mailto:do@presscom.pl). Pełna treść klauzuli informacyjnej dostępna jest na stronie internetowej: <https://presscom.pl/do>.

\_\_\_\_\_  
Data, pieczętka, podpis