URZĄD DOZORU TECHNICZNEGO

110 lat

Wspieramy rozwój
Dbamy o bezpieczeństwo

1911–2021

18.05.2021 | VII Konferencja Urzędu Dozoru Technicznego

TECHNIKA KSZTAŁTUJE ROZWÓJ

INNOWACJE W BEZPIECZEŃSTWIE
DLA PRZEMYSŁU XXI W.

FRAMEWORK UDT*Cyber*

Metodyka oceny organizacji – AUDYT CYBERBEZPIECZEŃSTWA

URZĄD DOZORU TECHNICZNEGO

110 lat

Wspieramy rozwój
Dbamy o bezpieczeństwo

1911–2021

18.05.2021 | VII Konferencja Urzędu Dozoru Technicznego

TECHNIKA KSZTAŁTUJE ROZWÓJ

INNOWACJE W BEZPIECZEŃSTWIE DLA PRZEMYSŁU XXI W.

PLAN PREZENTACJI

1. Wprowadzenie
2. Audyt cyberbezpieczeństwa
3. Framework UDT*Cyber* – struktura oraz zakres oceny
4. Zakres usług UDT-CERT w obszarze cyberbezpieczeństwa
5. Misja i wizja Urzędu Dozoru Technicznego w kontekście cyberbezpieczeństwa

CYBERBEZPIECZEŃSTWO – odporność systemów informacyjnych

na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy (UoKSC)

SYSTEMY KOMPUTEROWE

SECURITY

Przetwarzanie, przechowywanie, przesyłanie informacji

- seria norm ISO/IEC 27000
- Common Criteria (ISO 15408)

SAFETY

Sterowanie, podstawowe normy z zakresu bezpieczeństwa

- IEC 61508
- IEC 61511

Systemy komputerowe stosowane w organizacji powinny być zintegrowane w obszarze **SECURITY** oraz **SAFETY**.

Międzynarodowe standardy i metodyki

COBIT 5

ISO/IEC 27001

METODYKI

CPA – Cyber Program Assessment

NIST Cybersecurity Framework

Obowiązki Operatora Usługi Kluczowej

3 MIESĄCE

Wyznaczenie osoby kontaktowej
Szacowanie ryzyka
Zarządzanie incydentami
Obsługa incydentów
Zgłaszanie incydentów poważnych
Usuwanie podatności
Działania edukacyjne wobec użytkowników

6 MIESIĘCY

Wdrożenie odpowiednich środków technicznych i organizacyjnych
Zbieranie informacji o zagrożeniach i podatności
Zapobieganie i ograniczanie wpływu incydentów
Stosowanie wymaganej dokumentacji

12 MIESIĘCY

Pierwszy **audyt** w rozumieniu UoKSC
Przekazanie sprawozdania / raportu z audytu organowi właściwemu

Audyt Cyberbezpieczeństwa na zgodność z wymaganiami
Ustawy o Krajowym Systemie Cyberbezpieczeństwa
z dnia 5 lipca 2018 r.
– w oparciu o metodykę opisaną w dokumencie Framework UDT*Cyber*

! **OUK ma obowiązek stosowania odpowiedniej dokumentacji** wykorzystywanego do świadczenia usługi kluczowej (art.10.1 i 10.5 UoKSC)

! **OUK ma obowiązek przeprowadzić przeprowadzić pierwszy audyt bezpieczeństwa systemu informacyjnego** wykorzystywanego do świadczenia usługi kluczowej

! **OUK ma obowiązek zapewnić przeprowadzenie co najmniej raz na dwa lata audytu bezpieczeństwa systemu informacyjnego** wykorzystywanego do świadczenia usługi kluczowej

AUDYT CYBERBEZPIECZEŃSTWA

Audyt jest szczególnym przypadkiem badania systemu pod kątem zgodności z wymaganiami, wynika to z definicji zawartej w standardzie ISO/IEC 27000. Ustawa o Krajowym Systemie Cyberbezpieczeństwa definiuje natomiast

audyt cyberbezpieczeństwa operatora usługi kluczowej

jako systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia obowiązku prawnego wynikającego z ustawy.

Jak przejść przez audyt KSC spełniając tym samym obowiązki prawne wynikające z ustawy?

1. **FORMA PRZEPROWADZENIA AUDYTU**
   audytu nie da się przeprowadzić w formie zdalnej
2. **STOPIEŃ PRZYGOTOWANIA ORGANZIACJI**
   wynika to ze stanu/terminu wdrożenia systemu bezpieczeństwa
3. **POMYSŁ I SPOSÓB** na sprawne przeprowadzenie oceny
   odpowiedzią jest tutaj metodyka Framework UDT*Cyber*
4. **OCENA CAŁOŚCIOWA I KOMPLEKSOWA**
   w myśl zasady „*no safety without security*” oraz spełnienie wymagań UoKSC
5. **STANDARDY**
   ISO/IEC 27001 oraz ISO 22301

AUDYT CYBERBEZPIECZEŃSTWA

Audyt jest szczególnym rodzajem oceny wykonywanym przez

stronę niezależną

Niezależność musi być zachowana w stosunku do:

- organizacji/ zespołu projektowego lub np. budującego system zabezpieczeń;
- dostawców sprzętu i oprogramowania;
- organizacji podlegającej przeglądowi

(w skład zespołu audytowego nie mogą wchodzić pracownicy organizacji zlecającej audyt).

Podczas audytu należy ocenić:

zgodność dokumentacji, struktury, systemów informacyjnych z wymaganiami prawnymi i kryteriami audytu

- **Framework UDT*Cyber***

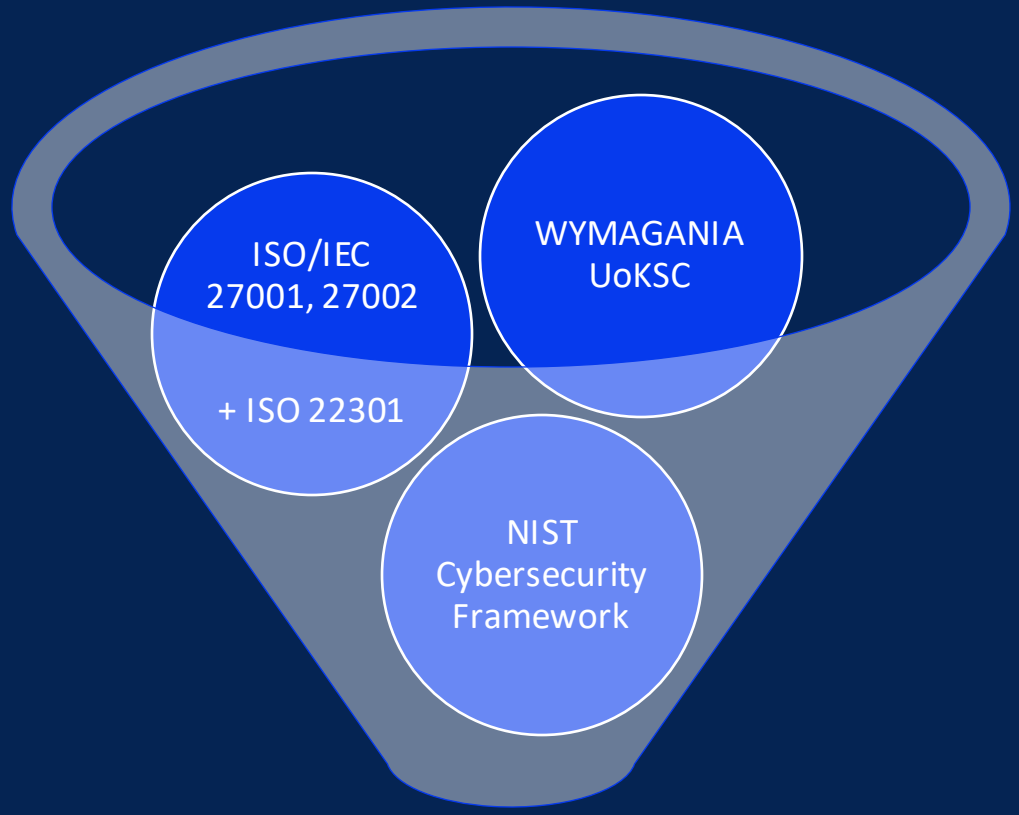
AUDYT CYBERBEZPIECZEŃSTWA

audyt cyberbezpieczeństwa

≠

przegląd według listy audytowej

FRAMEWORK UDT*Cyber*



FRAMEWORK UDT*Cyber*

FRAMEWORK UDT*Cyber*

MODUŁ 1
ORGANIZACJA

MODUŁ 2
OCHRONA

MODUŁ 3
KONTROLA

MODUŁ 4
REAGOWANIE

MODUŁ 5
PRZYWRACANIE DO DZIAŁANIA

MODUŁ 6
DOSKONALENIE

MODUŁ 7
OBOWIĄZKI OUK

FRAMEWORK UDT*Cyber*

MODUŁ 1

ORGANIZACJA

- **M1.1. STRUKTURA ORGANIZACYJNA I OTOCZENIE**
- **M1.2. ZASOBY LUDZKIE**
- **M1.3. ZARZĄDZANIE I ODPOWIEDZIALNOŚĆ**
- **M1.4. PRZYWÓDZTWO I ZAANGAŻOWANIE**
- **M1.5. STRATEGIE CYBERBEZPIECZEŃSTWA**
- **M1.6. SYSTEMY ZARZĄDZANIA**
- **M1.7. STANDARDY BEZPIECZEŃSTWA TECHNICZNEGO**

ZAKRES USŁUG

- **Audyt cyberbezpieczeństwa**
  w myśl Ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r.
- **Certyfikacja**
  - ✓ Systemów zarządzania bezpieczeństwem informacji PN-EN ISO/IEC 27001
  - ✓ Systemów zarządzania ciągłością działania - PN-EN ISO 22301
  - ✓ Systemów zarządzania bezpieczeństwem funkcjonalnym (ang. Functional Safety Management - FSM) PN-EN 61508, PN-EN 61511
- **Szkolenia**

DLACZEGO MY?

- **JEDNOSTKA AKREDYTOWANA**
  w ramach normy PN-EN ISO/IEC 27001
- **WYKWALIFIKOWNA KADRA**
  potencjał i możliwości realizacji zadań z obszaru cyberbezpieczeństwa
- **FRAMEWORK UDT*Cyber***
  podstawa do wdrożenia strategii cyberbezpieczeństwa w organizacji
- **MOŻLIWOŚCI TECHNICZNE**
  do przeprowadzania audytów cyberbezpieczeństwa i **niezbędną wiedzą** w wymaganym obszarze

POLSKIE CENTRUM AKREDYTACJI
POLISH CENTRE FOR ACCREDITATION

CERTYFIKAT AKREDYTACJI
JEDNOSTKI CERTYFIKUJĄCEJ
SYSTEMY ZARZĄDZANIA
ACCREDITATION CERTIFICATE FOR MANAGEMENT SYSTEMS CERTIFICATION BODY
Nr AC 078

URZĄD DOZORU TECHNICZNEGO
Jednostka Certyfikująca Systemy Zarządzania UDT-Cert
ul. Szczęśliwicka 34, 02-353 Warszawa

spełnia wymagania normy PN-EN ISO/IEC 17021-1:2015-09

Akredytowana działalność jest określona w Zakresie Akredytacji Nr AC 078

Akredytacja pozostaje w mocy pod warunkiem przestrzegania wymagań jednostki akredytującej określonych w kontrakcie Nr AC 078

Akredytację udzielono dnia 01.12.2000 r.

DYREKTOR POLSKIEGO CENTRUM AKREDYTACJI
LUCYNA GLIBORSKA

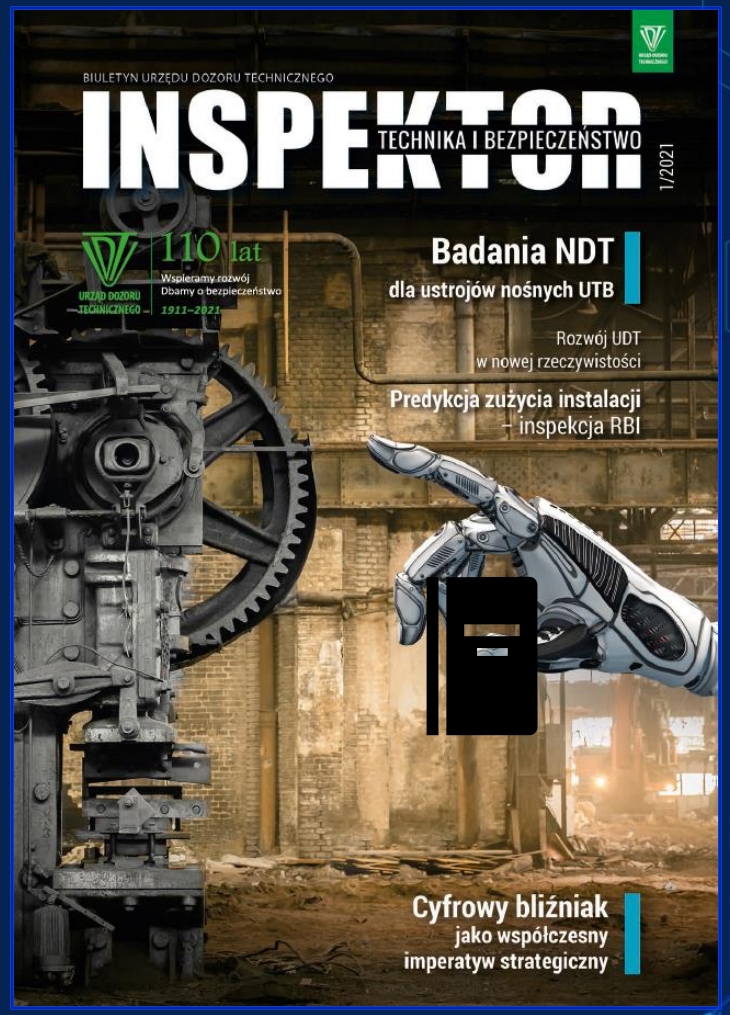
Warszawa, 29 listopada 2019 roku

MISJA I WIZJA UDT

Misją Urzędu Dozoru Technicznego
jest **wspieranie rozwoju i dbanie o bezpieczeństwo**
zgodnie z obowiązującą wizją:
Lider innowacyjności w obszarze bezpieczeństwa publicznego
w tym również w obszarze cyberbezpieczeństwa.

BEZPIECZEŃTWO – PROCES – CIĄGŁA TRANSFORMACJA

Bezpieczeństwo to proces, który musi być doskonalony by funkcjonował skutecznie



Dziękuję za uwagę

URZĄD DOZORU TECHNICZNEGO

110 lat

Wspieramy rozwój
Dbamy o bezpieczeństwo

1911–2021

18.05.2021 | VII Konferencja Urzędu Dozoru Technicznego

TECHNIKA KSZTAŁTUJE ROZWÓJ

INNOWACJE W BEZPIECZEŃSTWIE DLA PRZEMYSŁU XXI W.

DOROTA BAŁACHOWSKA

DANE KONTAKTOWE:

Numer telefonu: +48 883 375 856

E-mail: dorota.balachowska@udt.gov.pl
cybersecurity@udt.gov.pl

Informacje dodatkowe:

Departament Certyfikacji i Oceny Zgodności UDT-CERT

Zespół ds. Cyberbezpieczeństwa UDT

Auditor wiodący na zgodność z UoKSC