Proaktywne Kierownictwo

Czyli co Zarząd musi wiedzieć?
Co musi robić?
A co może delegować?

Arcus SECURE DAY

one step ahead sagenso

Bartosz Kozłowski

Ekspert ds. cyberbezpieczeństwa
CEH, CISA, CISM, CRISC

Odpowiedzialny za realizację setek projektów z zakresu zarządzania bezpieczeństwem IT w ramach KPMG m.in. dla banków i towarzystw ubezpieczeniowych (2010-2016) a także za stworzenie i prowadzenie działu cyberbezpieczeństwa w PLL LOT S.A.(2016 – 2019). Obecnie konsultant ds. bezpieczeństwa systemów teleinformatycznych w biznesie (audyty, informatyka śledcza, testy penetracyjne, zarządzanie ryzykiem) i Chief Security Officer w Sagenso, dynamicznie rozwijającej się spółce z branży cyberbezpieczeństwa, która już zdobyła uznanie takich partnerów jak: NCBR, PAIH, PARP, SAMSUNG i MICROSOFT.

Co Zarząd **musi wiedzieć**?

Bezpieczeństwo IT **to nie jest odpowiedzialność IT**

Kopalnia Wiedzy.pl

wpisz szukaną frazę

Wiadomości | Artykuły | Forum | Książki | Konkursy | Galerie | Wywi

Medycyna | Technologia | Psychologia | Zdrowie/uroda | Bezpieczeństwo IT | Nauki przyrodnicze | Astronomia/fizyka | Humar

Strona główna > Wiadomości > Bezpieczenstwo IT

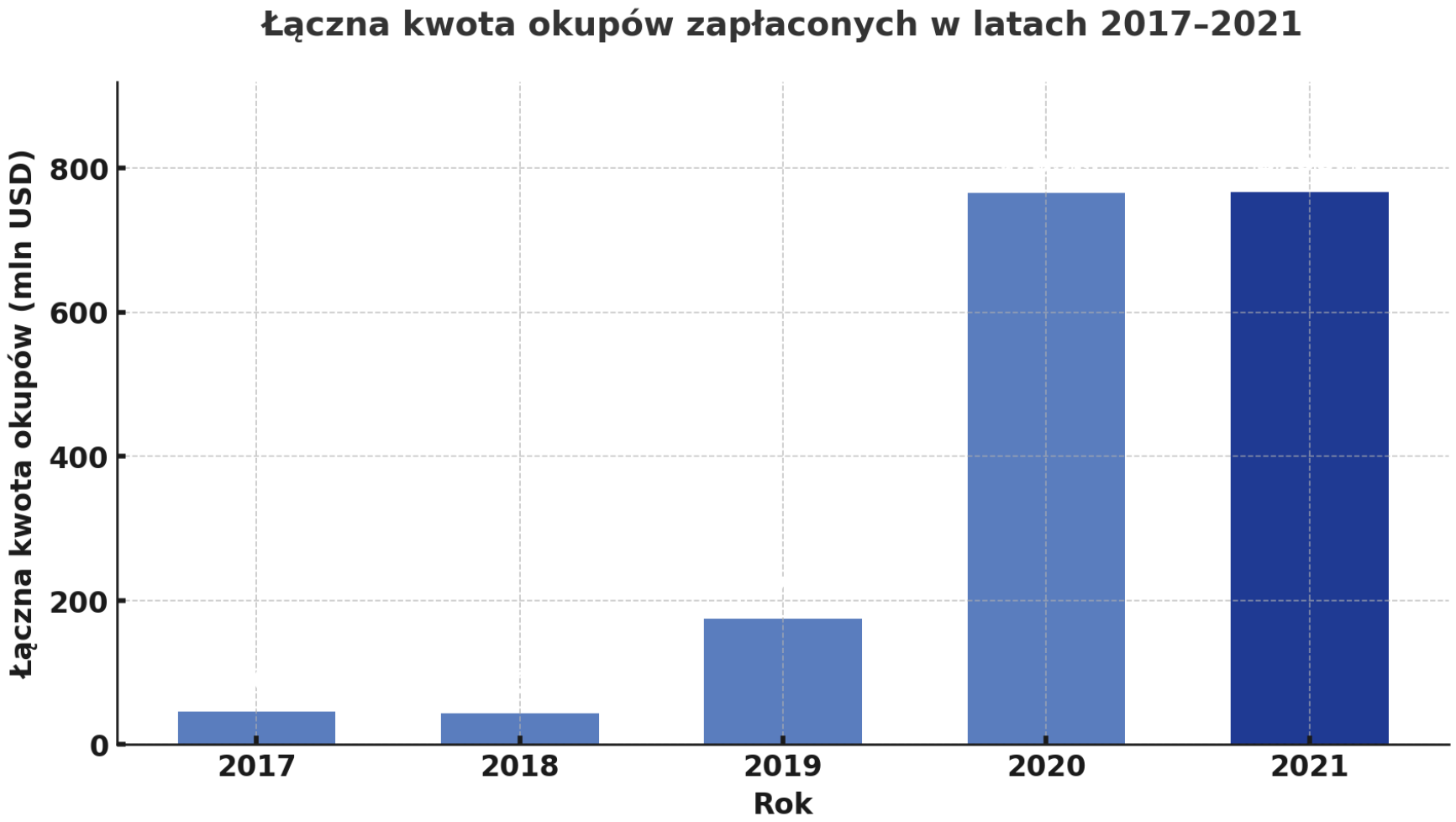
Rosjanie próbowali zaatakować Teslę. Firmie Muska pomógł nieprzekupny pracownik i FBI

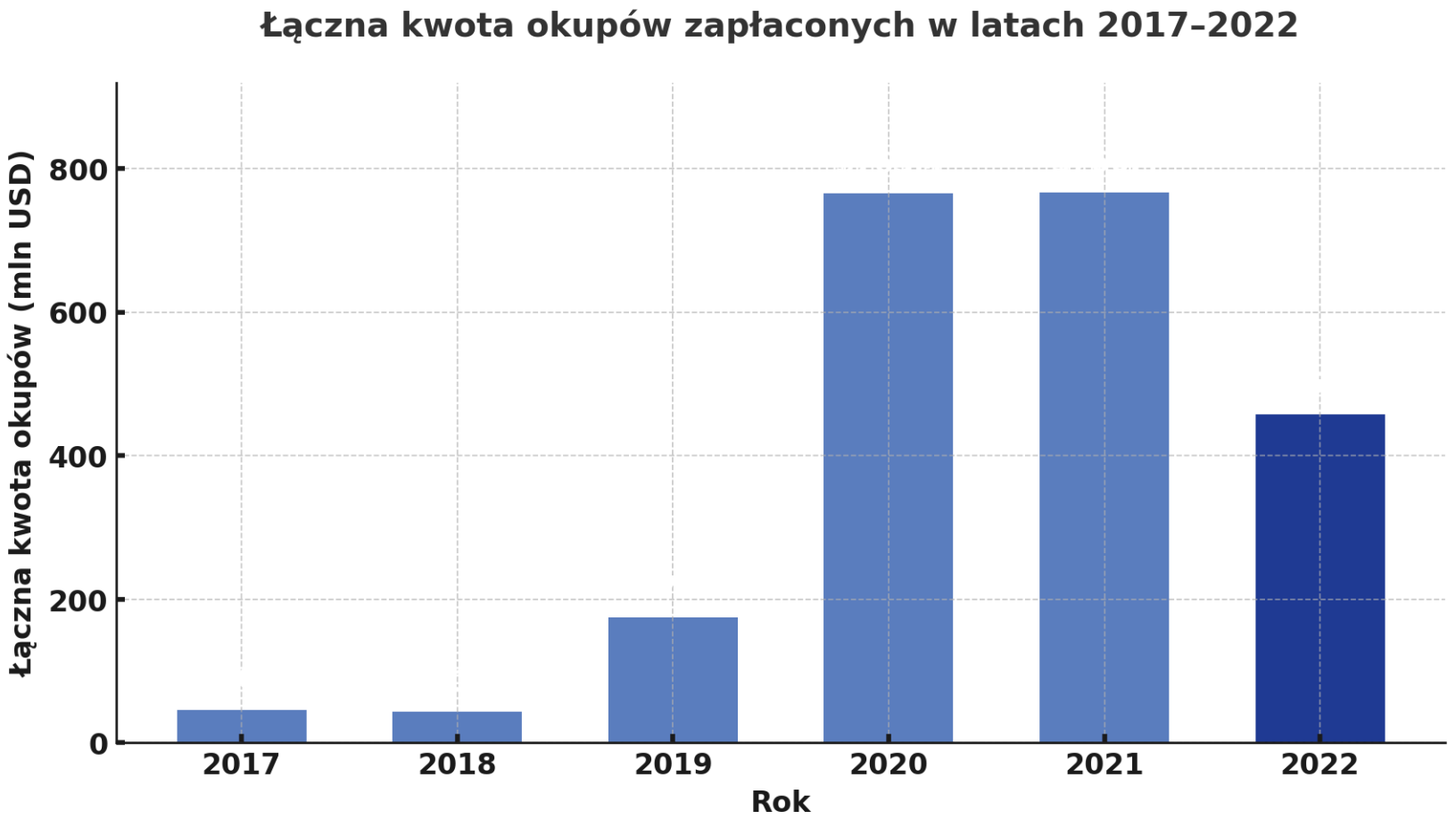
A A A

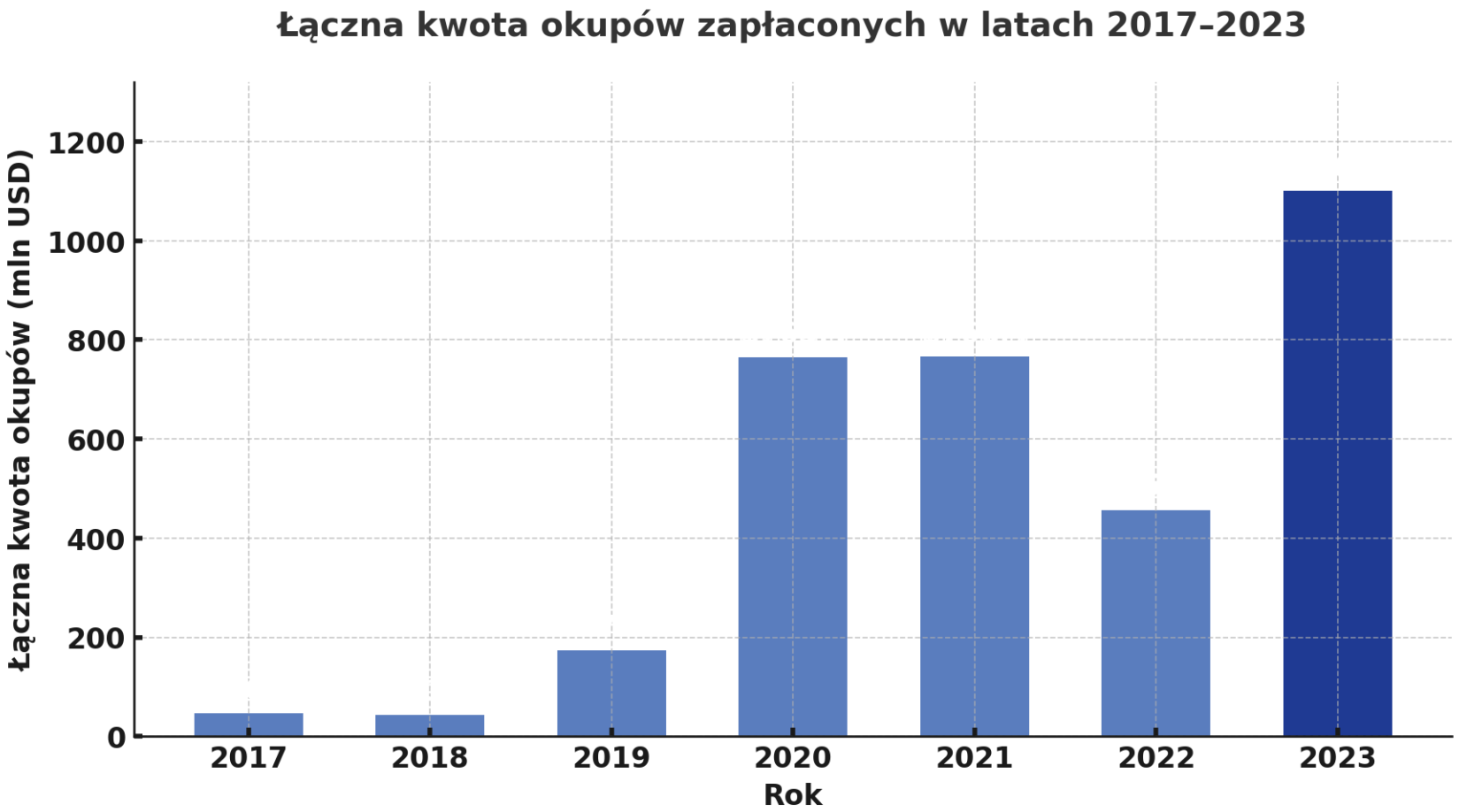
29 sierpnia 2020, 11:19 | Bezpieczenstwo IT

Elon Musk potwierdził, że **rosyjski cyberprzestępca próbował przekupić jednego z pracowników firmy, by ten zainstalował ransomware w sieci firmowej Gigafactory** w Newadzie. Próbę ataku podjął 27-letni Jegor Igorewicz Kriuczkow, który zaoferował anonimowemu pracownikowi Tesli milion dolarów za zainfekowanie systemu. Jeśli do infekcji by doszło, Kriuczkow i jego wspólnicy mogliby przeprowadzić atak DDoS na system Tesli.

Szczegóły całej operacji poznaliśmy dzięki dokumentom ujawnionym przez FBI po aresztowaniu Kriuczkowa. Z dokumentów wynika, że Kriuczkow przyjechał do USA jako turysta w lipcu bieżącego roku. Wybrał się do miejscowości Sparks w


Łączna kwota okupów zapłaconych w latach 2017–2021
Łączna kwota okupów (mln USD)
0
200
400
600
800
2017
2018
2019
2020
2021
Rok


Łączna kwota okupów zapłaconych w latach 2017–2022
Łączna kwota okupów (mln USD)
0
200
400
600
800
2017
2018
2019
2020
2021
2022
Rok


Łączna kwota okupów zapłaconych w latach 2017–2023
Łączna kwota okupów (mln USD)
0
200
400
600
800
1000
1200
2017
2018
2019
2020
2021
2022
2023
Rok

CyberDefence 24

ARMIA I SŁUŻBY | POLITYKA I PRAWO | CYBERBEZPIECZEŃSTWO | STREFA BANKU P

BIZNES I FINANSE | SOCIAL MEDIA | #CYBERMAGAZYN | TECHNOLOGIE | PRYWATY

CYBERBEZPIECZEŃSTWO

Ataki na NATO i wojsko USA. Zatrzymano hakera

SZYMON PALCZEWSKI
06.02.2025 09:54

DRUKUJ PDF

Siły Zbrojne Hiszpanii

Autor. Ministerio Defensa (@Defensagob)/X

Bankier.pl • Biznes • Technologia • Wiadomości

Atak na bazy danych NATO. Okazało się, że hakerem jest 18-latek z Hiszpanii

publikacja 2025-02-05 20:28

aktualizacja 2025-02-06 07:28

Hiszpańska policja poinformowała w środę o zatrzymaniu 18-letniego hackera, który przeprowadził ponad 40 cyberataków na strategiczne instytucje krajowe i międzynarodowe, w tym bazy danych NATO.

„Zarządzający firmami obecnie powszechnie akceptują, że
cyberzagrożenia są głównym ryzykiem biznesowym, którym należy zarządzać,
a nie problemem technologicznym do rozwiązania„

*Gartner: „**Gartner Identifies the Top Cybersecurity Trends for 2023**”*

Ustawa o KSC:

Jeśli **kierownik danego podmiotu** „nie dochowa należytej staranności celem spełnienia obowiązków” **może otrzymać on dodatkową karę pieniężną nieprzekraczającą 200% jego miesięcznego wynagrodzenia.**

Co Zarząd **musi robić**?

Zarząd musi **proaktywnie zarządzać**

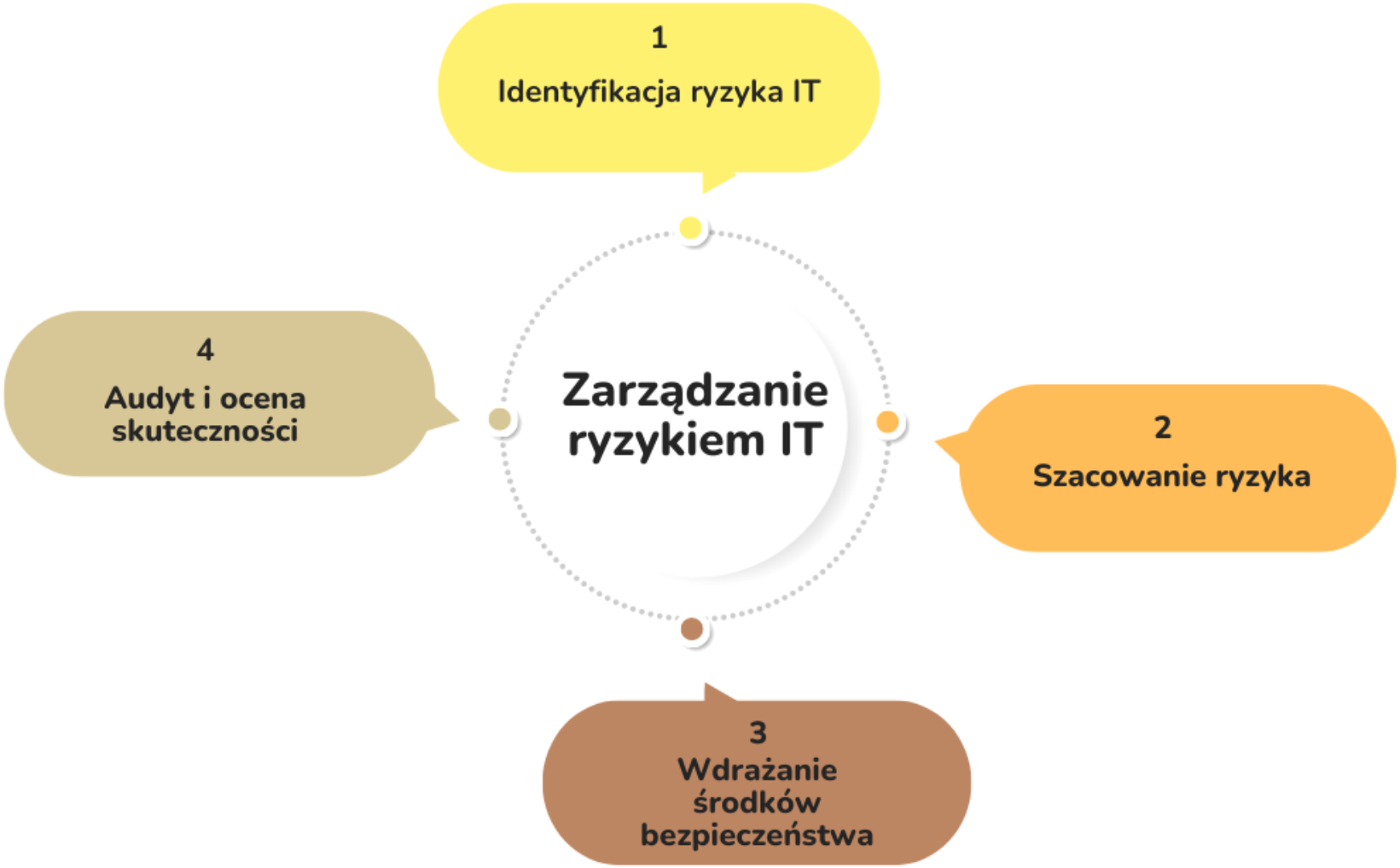
ryzykiem technologicznym

Ustawa o KSC:

Jeśli kierownik danego podmiotu „**nie dochowa należytej staranności celem spełnienia obowiązków**” może otrzymać on dodatkową karę pieniężną nieprzekraczającą 200% jego miesięcznego wynagrodzenia.

Kara ta może być przyznana także, jeśli organ właściwy uzna, że stoją za tym przesłanki wynikające z **czasu trwania**, **zakresu** lub **skutków naruszenia**.

Przykład: ISO 27001
Polityki bezpieczeństwa danych
Organizacja bezpieczeństwa informacji
Bezpieczeństwo zasobów ludzkich
Zarządzanie aktywami
Kontrola dostępu
Kryptografia
Bezpieczeństwo fizyczne i środowiskowe
Bezpieczna eksploatacja
Bezpieczeństwo komunikacji
Pozyskiwanie, rozwój i utrzymanie systemów
Relacje z dostawcami
Zarządzanie incydentami
BCM - zapewnienie ciągłości działania
Zgodność


1
Identyfikacja ryzyka IT
2
Szacowanie ryzyka
3
Wdrażanie środków bezpieczeństwa
4
Audyt i ocena skuteczności
Zarządzanie ryzykiem IT

Co Zarząd musi robić?

- **Szacować ryzyko technologiczne** dla operacji biznesowych
- **Wdrożyć sformalizowane zasady** zarządzania bezpieczeństwem IT
- **Nadzorować** kluczowe wskaźniki efektywności (KPI) i zagrożeń (KRI)
- **Systematycznie audytować skuteczność**, w razie potrzeby udoskonalać

Co Zarząd **może delegować?**

Prawie **wszystko.**

TVP info_

TYLKO U NAS

Jak randkują Polacy? Sposobów na poznawanie nowych osób jest bez liku

Pierwsze takie starcie w historii. Pilot myśliwca zmierzył się ze sztuczną inteligencją

KM 20.04.2024, 06:48 / aktualizacja: 07:02

Udostępnij:

DARPA przeprowadziła testowe starcie ludzkiego pilota ze sztuczną inteligencją (fot. Aytac Unal/Anadolu Agency via Getty Images)

Laser z AI w Szpitalu Kolejowym w Katowicach operuje jaskrę w nieco ponad dwie sekundy! Nowy sprzęt w klinice

Mateusz Czajka
11 czerwca 2024, 12:35

Udostępnij

ZET WIADOMOŚCI NEWS POLSKA ŚWIAT POLITYKA BIZNES SPORT WIĘCEJ

Radio ZET ▸ Wiadomości ▸ Świat ▸ Izrael wykorzystuje AI do kierowania atakami? Ofiary wśród cywilów "wliczone w koszta

Obserwuj w Google News

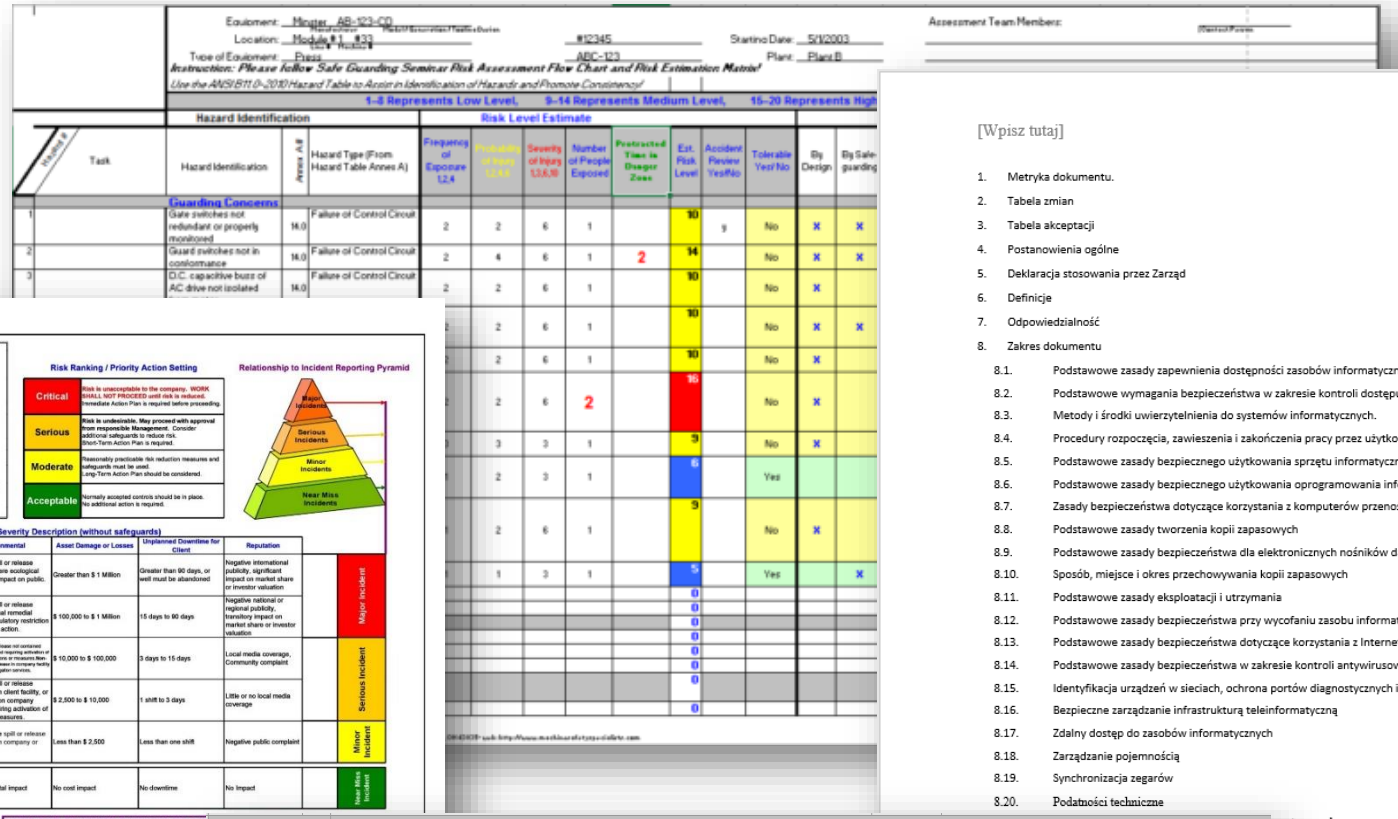
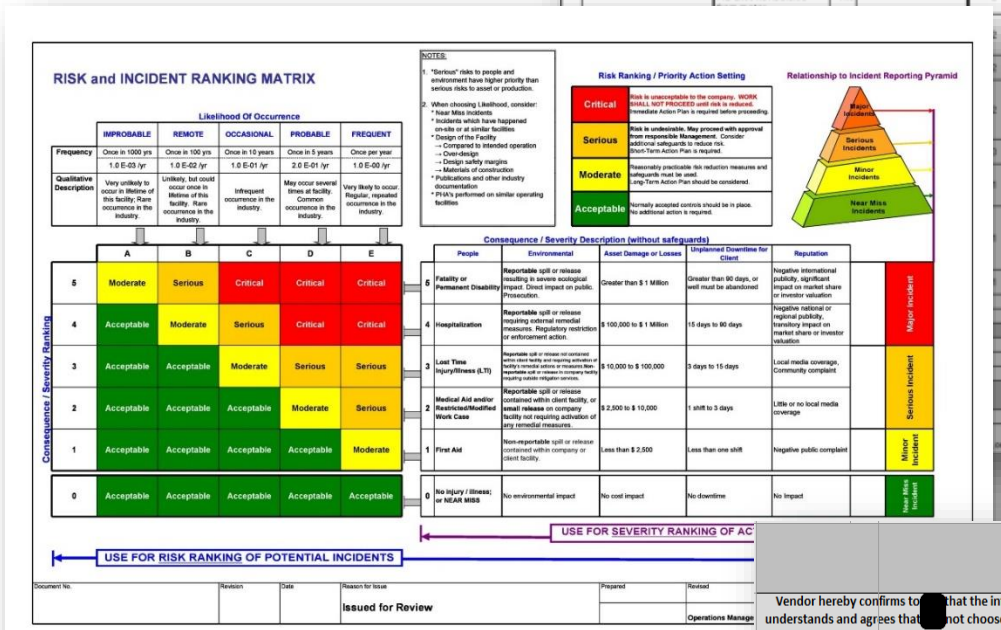
Izrael wykorzystuje AI do kierowania atakami? Ofiary wśród cywilów "wliczone w koszta"

Mateusz Stelmaszczyk
2 min. czytania | 05.04.2024 10:08

PODZIEL SIĘ

W mediach pojawił się szokujący przeciek. Wynika z niego, że armia Izraela może wykorzystywać sztuczną inteligencję do kierowania atakami w Strefie Gazy. Przerażające jest to, że ofiary wśród cywilów mają być rzekomo "wliczone w koszta" takich ataków.

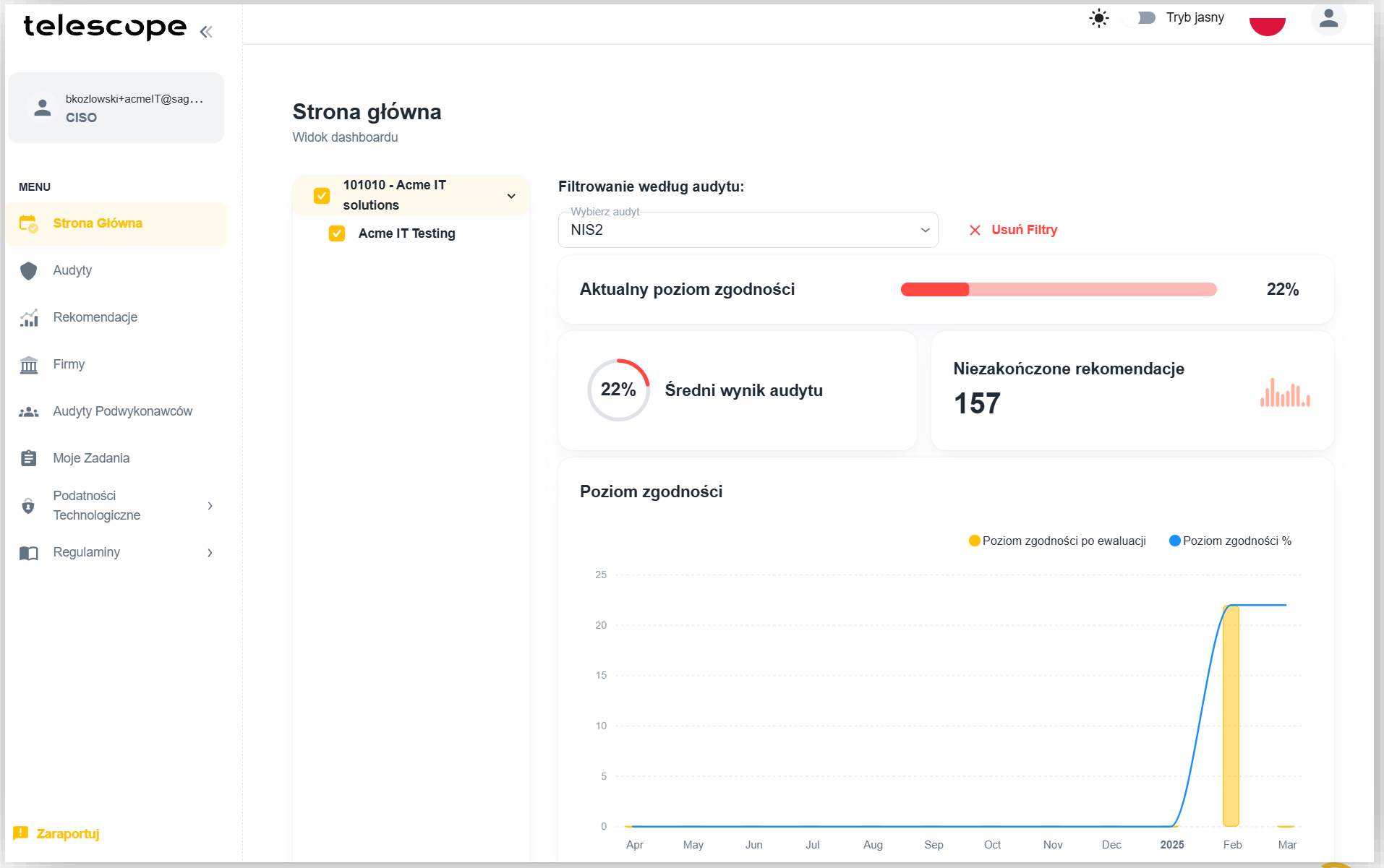

HUMANITY:
GAME OVER

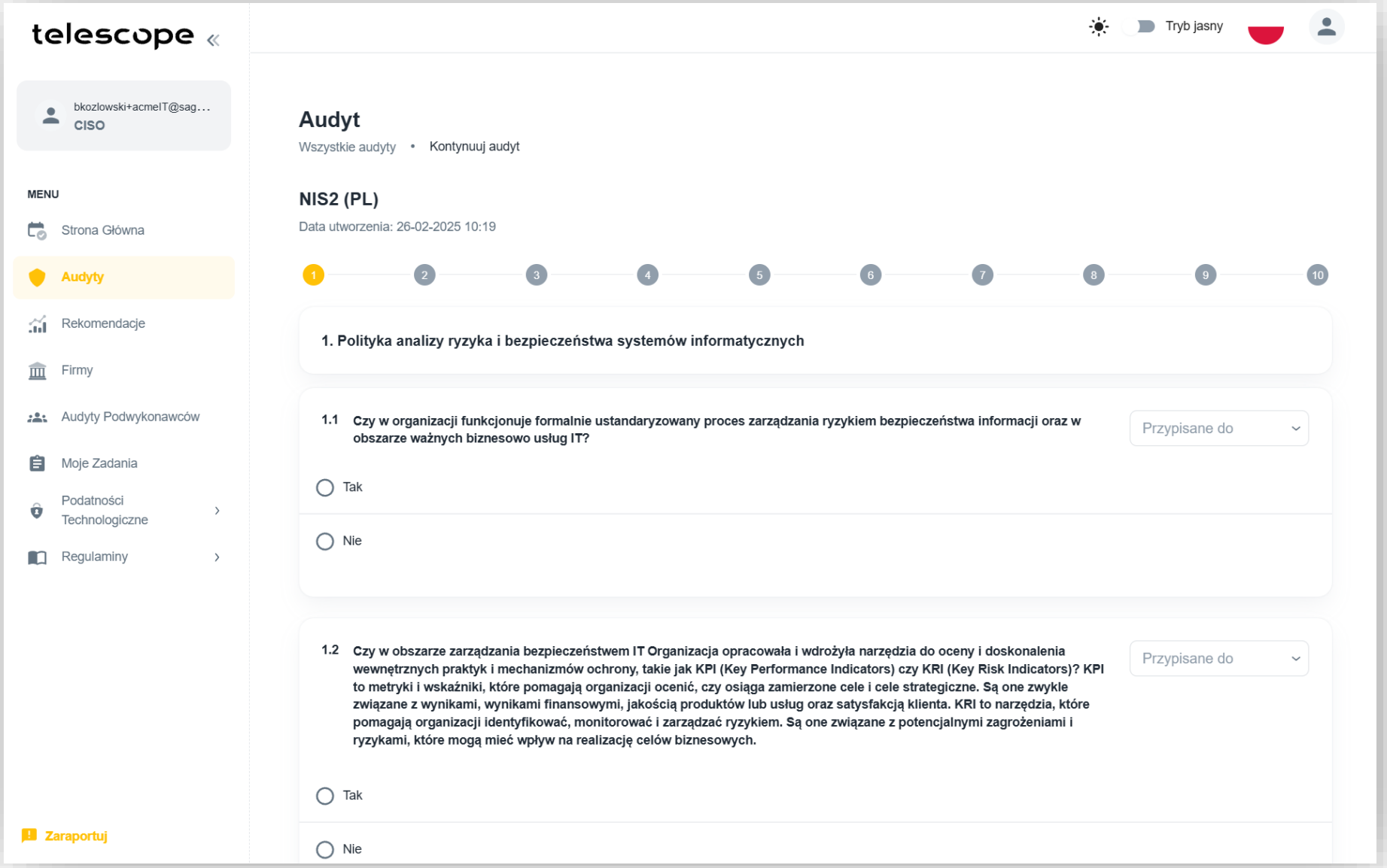

Equipment: Mixer AB-123-CD
Location: Module # 1 #33
Type of Equipment: Press
#12345
ABC-123
Starting Date: 5/1/2003
Plant: Plant B
Assessment Team Members:
Instruction: Please follow Safe Guarding Seminar Risk Assessment Flow Chart and Risk Estimation Matrix!
Use the ANSI B11.0-2010 Hazard Table to Assist in Identification of Hazards and Promote Consistency!
1-8 Represents Low Level, 9-14 Represents Medium Level, 15-20 Represents High
Hazard Identification
Risk Level Estimate
Task
Hazard Identification
Annex A-B
Hazard Type (From Hazard Table Annex A)
Frequency of Exposure 1,2,4
Probability of Injury 1,2,4,8
Severity of Injury 1,3,6,10
Number of People Exposed
Protracted Time in Danger Zone
Est. Risk Level
Accident Review Yes/No
Tolerable Yes/ No
By Design
By Safe-guarding
Guarding Concerns
Gate switches not redundant or properly monitored
14.0
Failure of Control Circuit
Guard switches not in conformance
14.0
Failure of Control Circuit
D.C. capacitive buss of AC drive not isolated
14.0
Failure of Control Circuit

RISK and INCIDENT RANKING MATRIX
Likelihood Of Occurrence
IMPROBABLE
REMOTE
OCCASIONAL
PROBABLE
FREQUENT
Frequency
Once in 1000 yrs
Once in 100 yrs
Once in 10 years
Once in 5 years
Once per year
1.0 E-03 /yr
1.0 E-02 /yr
1.0 E-01 /yr
2.0 E-01 /yr
1.0 E-00 /yr
Qualitative Description
Very unlikely to occur in lifetime of this facility; Rare occurrence in the industry.
Unlikely, but could occur once in lifetime of this facility. Rare occurrence in the industry.
Infrequent occurrence in the industry.
May occur several times at facility. Common occurrence in the industry.
Very likely to occur. Regular, repeated occurrence in the industry.
Consequence / Severity Ranking
A
B
C
D
E
5 Moderate Serious Critical Critical Critical
4 Acceptable Moderate Serious Critical Critical
3 Acceptable Acceptable Moderate Serious Serious
2 Acceptable Acceptable Acceptable Moderate Serious
1 Acceptable Acceptable Acceptable Acceptable Moderate
0 Acceptable Acceptable Acceptable Acceptable Acceptable
NOTES:
1. "Serious" risks to people and environment have higher priority than serious risks to asset or production.
2. When choosing Likelihood, consider:
* Near Miss Incidents
* Incidents which have happened on-site or at similar facilities
* Design of the Facility
→ Compared to intended operation
→ Over-design
→ Design safety margins
→ Materials of construction
* Publications and other industry documentation
* PHA's performed on similar operating facilities
Risk Ranking / Priority Action Setting
Critical
Risk is unacceptable to the company. WORK SHALL NOT PROCEED until risk is reduced. Immediate Action Plan is required before proceeding.
Serious
Risk is undesirable. May proceed with approval from responsible Management. Consider additional safeguards to reduce risk. Short-Term Action Plan is required.
Moderate
Reasonably practicable risk reduction measures and safeguards must be used. Long-Term Action Plan should be considered.
Acceptable
Normally accepted controls should be in place. No additional action is required.
Relationship to Incident Reporting Pyramid
Major Incidents
Serious Incidents
Minor Incidents
Near Miss Incidents
Consequence / Severity Description (without safeguards)
People
Environmental
Asset Damage or Losses
Unplanned Downtime for Client
Reputation
5 Fatality or Permanent Disability — Reportable spill or release resulting in severe ecological impact. Direct impact on public. Prosecution. — Greater than $ 1 Million — Greater than 90 days, or well must be abandoned — Negative international publicity, significant impact on market share or investor valuation
4 Hospitalization — Reportable spill or release requiring external remedial measures. Regulatory restriction or enforcement action. — $ 100,000 to $ 1 Million — 15 days to 90 days — Negative national or regional publicity, transitory impact on market share or investor valuation
3 Lost Time Injury/Illness (LTI) — Reportable spill or release not contained within client facility and requiring activation of facility's remedial actions or measures.Non-reportable spill or release contained within facility requiring outside mitigation services. — $ 10,000 to $ 100,000 — 3 days to 15 days — Local media coverage, Community complaint
2 Medical Aid and/or Restricted/Modified Work Case — Reportable spill or release contained within client facility, or small release on company facility not requiring activation of any remedial measures. — $ 2,500 to $ 10,000 — 1 shift to 3 days — Little or no local media coverage
1 First Aid — Non-reportable spill or release contained within company or client facility. — Less than $ 2,500 — Less than one shift — Negative public complaint
0 No Injury / Illness; or NEAR MISS — No environmental impact — No cost impact — No downtime — No Impact
Major Incident
Serious Incident
Minor Incident
Near Miss Incident
USE FOR SEVERITY RANKING OF AC
USE FOR RISK RANKING OF POTENTIAL INCIDENTS
Document No.
Revision
Date
Reason for Issue
Issued for Review
Prepared
Revised
Operations Manage
[redacted] Vendor Checklist
[redacted] - Lista kontrolna dostawcy
Vendor hereby confirms to [redacted] that the information provided based on the cheklist below are accurate and reflect the true situation. If some of the answers are not accurate or do not reflect the t
understands and agrees that [redacted] not choose the Vendor, may terminate the contractual relationship with Vendor at [redacted] earliest convenience without [redacted] being liable to Vendor for any form of co
otherwise).
Dostawca niniejszym potwierdza [redacted], że informacje udzielone na podstawie poniższej listy są poprawne i odzwierciedlają prawdziwą sytuację. Jeżeli którekolwiek odpowiedzi okażą się niepoprawne
może nie dokonać wyboru dostawcy, rozwiązać umowę z dostawcą w trybie natychmiastowym, nie ponosząc wobec Dostawcy jakiejkolwiek odpowiedzialności czy jakiejkolwiek formy rekompensat
Section
Obszar
Question
Pytanie
YES / NO
TAK / N
Answer
Odpowiedź
Vendor Security Policy
Polityka bezpieczeństwa dostawcy
31
Is there a regular review and approval process for this policy?
Czy jest przeprowadzana regularna aktualizacja i proces zatwierdzania tej polityki?
YES - TAK
Justify your answer here / Uzasadnij swoją odpowiedź poniżej
Co najmniej raz w roku.
32
When an employee, consultant, subcontractor, vendor or other third party service provider is terminated, is their physical and electronic access to entrusted personal data terminated immediately?
[This includes deactivating passwords and user names]
Czy w przypadku zakończenia umowy z pracownikiem, konsultantem, podwykonawcą dostawcy lub z innym podwykonawcom, fizyczny i elektroniczny dostęp do powierzonych danych osobowych jest odbierany natychmiast po zakończeniu umowy?
[W tym poprzez dezaktywację haseł i nazw użytkowników]
YES - TAK
Justify your answer here / Uzasadnij swoją odpowiedź poniżej
Najpóźniej z datą wygaśnięcia umowy.
[Wpisz tutaj]

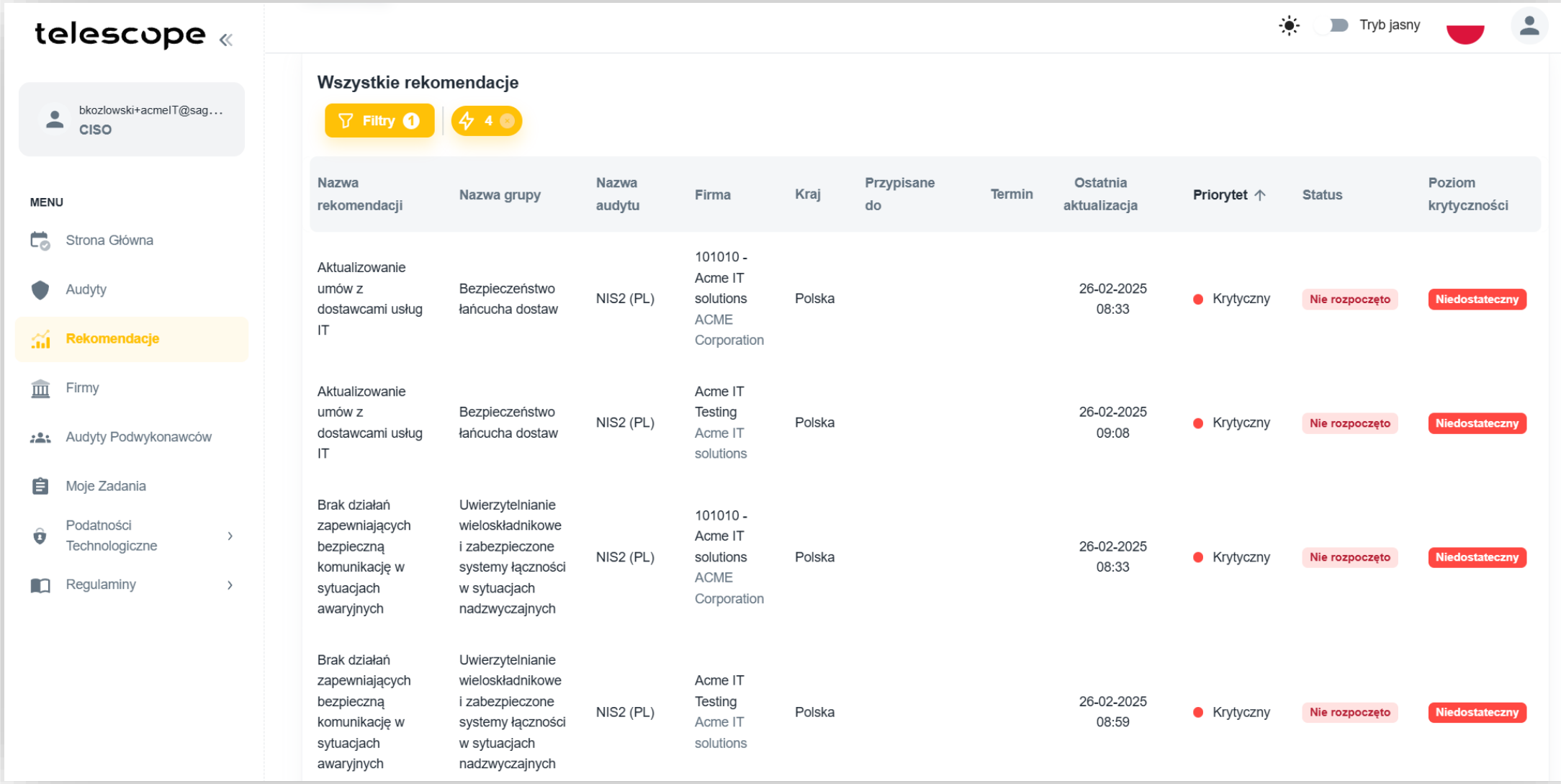
arcus

telescope

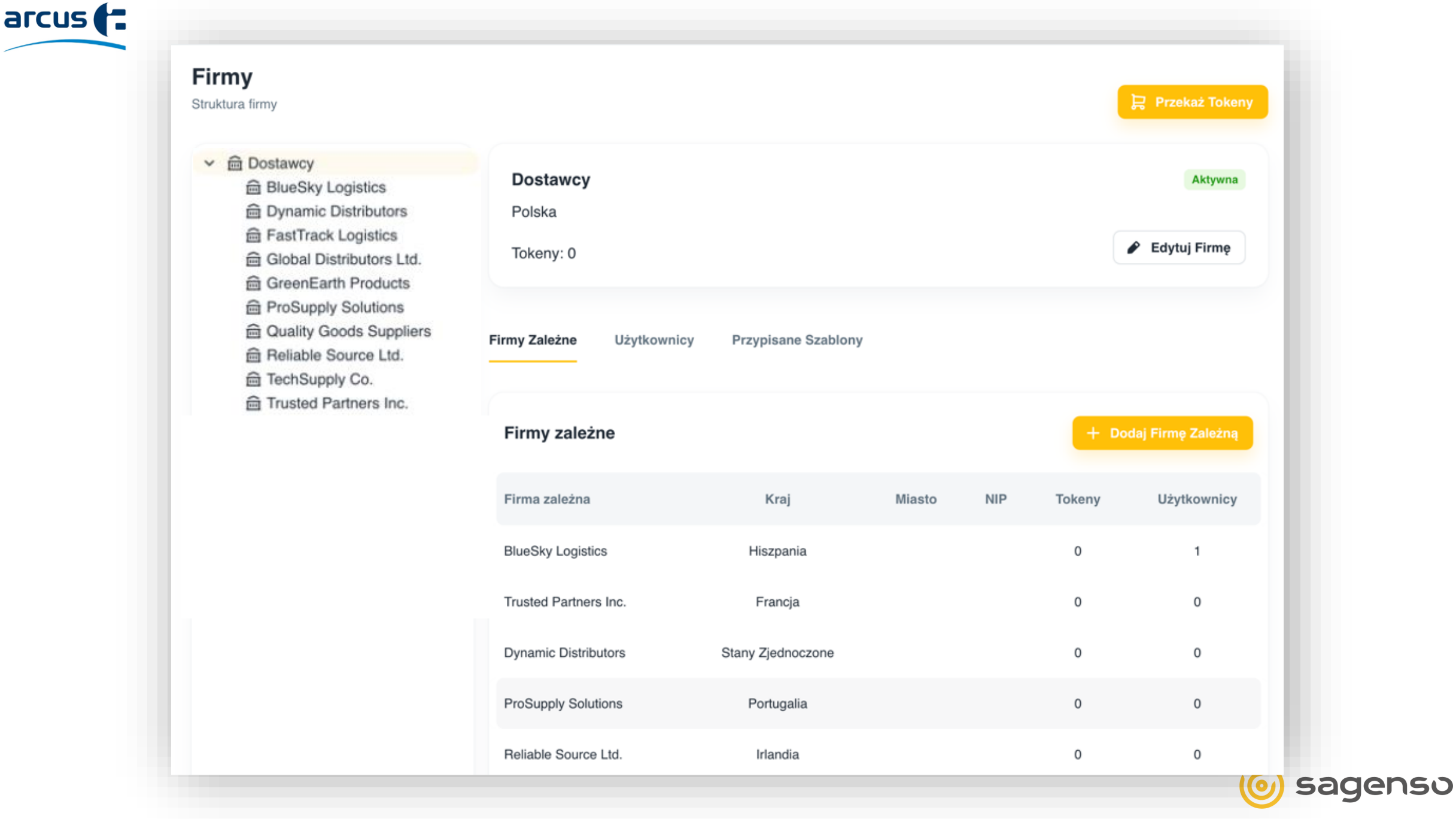
sagenso

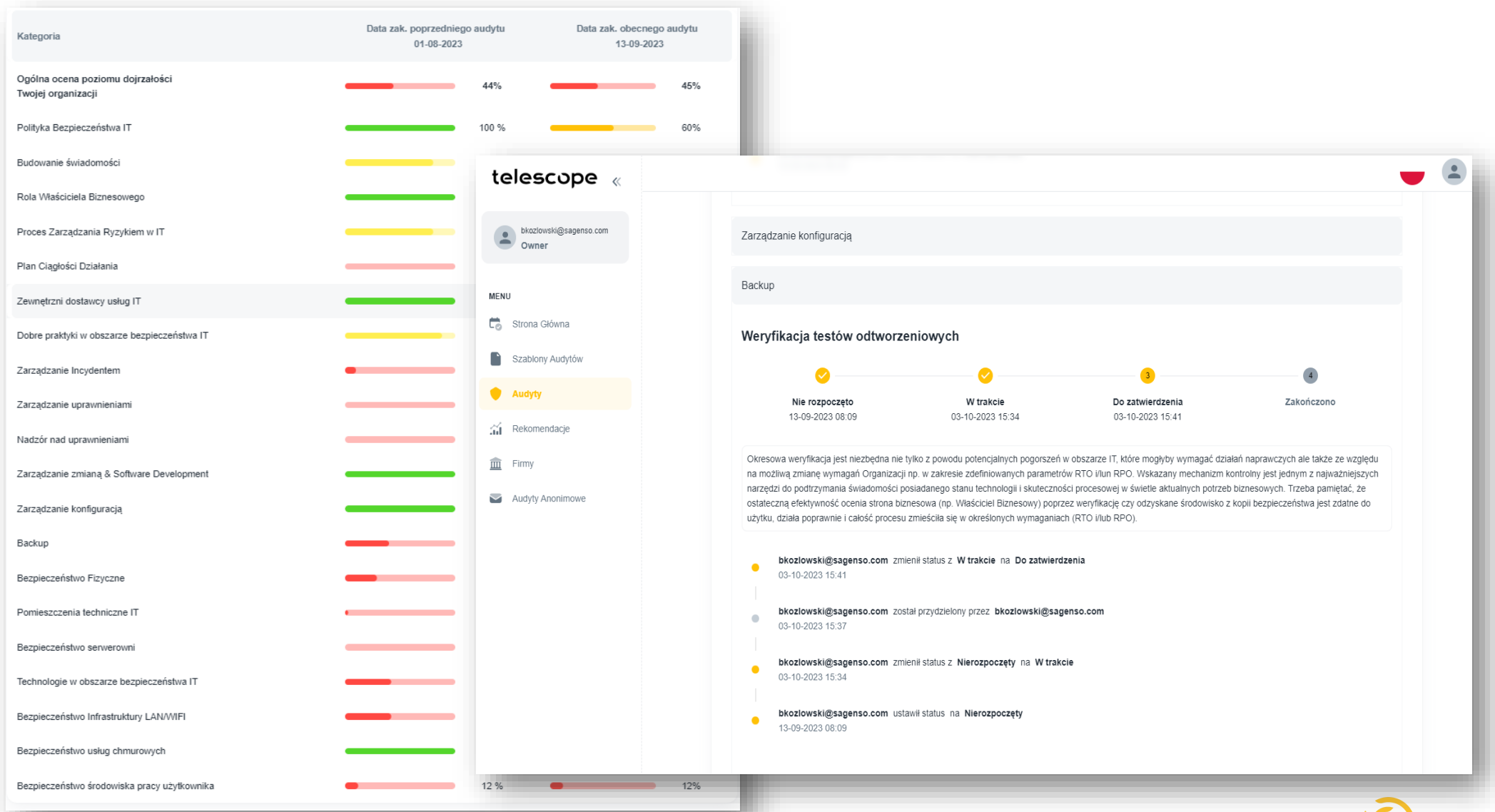

telescope
Tryb jasny
bkozlowski+acmeIT@sag...
CISO
MENU
Strona Główna
Audyty
Rekomendacje
Firmy
Audyty Podwykonawców
Moje Zadania
Podatności Technologiczne
Regulaminy
Zaraportuj
Strona główna
Widok dashboardu
101010 - Acme IT solutions
Acme IT Testing
Filtrowanie według audytu:
Wybierz audyt
NIS2
Usuń Filtry
Aktualny poziom zgodności
22%
22%
Średni wynik audytu
Niezakończone rekomendacje
157
Poziom zgodności
Poziom zgodności po ewaluacji
Poziom zgodności %
25
20
15
10
5
0
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
2025
Feb
Mar


telescope
bkozlowski+acmeIT@sag...
CISO
MENU
Strona Główna
Audyty
Rekomendacje
Firmy
Audyty Podwykonawców
Moje Zadania
Podatności Technologiczne
Regulaminy
Zaraportuj
Tryb jasny
Audyt
Wszystkie audyty • Kontynuuj audyt
NIS2 (PL)
Data utworzenia: 26-02-2025 10:19
1 2 3 4 5 6 7 8 9 10
1. Polityka analizy ryzyka i bezpieczeństwa systemów informatycznych
1.1 Czy w organizacji funkcjonuje formalnie ustandaryzowany proces zarządzania ryzykiem bezpieczeństwa informacji oraz w obszarze ważnych biznesowo usług IT?
Przypisane do
Tak
Nie
1.2 Czy w obszarze zarządzania bezpieczeństwem IT Organizacja opracowała i wdrożyła narzędzia do oceny i doskonalenia wewnętrznych praktyk i mechanizmów ochrony, takie jak KPI (Key Performance Indicators) czy KRI (Key Risk Indicators)? KPI to metryki i wskaźniki, które pomagają organizacji ocenić, czy osiąga zamierzone cele i cele strategiczne. Są one zwykle związane z wynikami, wynikami finansowymi, jakością produktów lub usług oraz satysfakcją klienta. KRI to narzędzia, które pomagają organizacji identyfikować, monitorować i zarządzać ryzykiem. Są one związane z potencjalnymi zagrożeniami i ryzykami, które mogą mieć wpływ na realizację celów biznesowych.
Przypisane do
Tak
Nie



Nazwa rekomendacji	Nazwa grupy	Nazwa audytu	Firma	Kraj	Przypisane do	Termin	Ostatnia aktualizacja	Priorytet	Status	Poziom krytyczności
Aktualizowanie umów z dostawcami usług IT	Bezpieczeństwo łańcucha dostaw	NIS2 (PL)	101010 - Acme IT solutions ACME Corporation	Polska			26-02-2025 08:33	Krytyczny	Nie rozpoczęto	Niedostateczny
Aktualizowanie umów z dostawcami usług IT	Bezpieczeństwo łańcucha dostaw	NIS2 (PL)	Acme IT Testing Acme IT solutions	Polska			26-02-2025 09:08	Krytyczny	Nie rozpoczęto	Niedostateczny
Brak działań zapewniających bezpieczną komunikację w sytuacjach awaryjnych	Uwierzytelnianie wieloskładnikowe i zabezpieczone systemy łączności w sytuacjach nadzwyczajnych	NIS2 (PL)	101010 - Acme IT solutions ACME Corporation	Polska			26-02-2025 08:33	Krytyczny	Nie rozpoczęto	Niedostateczny
Brak działań zapewniających bezpieczną komunikację w sytuacjach awaryjnych	Uwierzytelnianie wieloskładnikowe i zabezpieczone systemy łączności w sytuacjach nadzwyczajnych	NIS2 (PL)	Acme IT Testing Acme IT solutions	Polska			26-02-2025 08:59	Krytyczny	Nie rozpoczęto	Niedostateczny


Firmy
Struktura firmy
Przekaż Tokeny
Dostawcy
BlueSky Logistics
Dynamic Distributors
FastTrack Logistics
Global Distributors Ltd.
GreenEarth Products
ProSupply Solutions
Quality Goods Suppliers
Reliable Source Ltd.
TechSupply Co.
Trusted Partners Inc.
Dostawcy
Aktywna
Polska
Tokeny: 0
Edytuj Firmę
Firmy Zależne
Użytkownicy
Przypisane Szablony
Firmy zależne
Dodaj Firmę Zależną
Firma zależna
Kraj
Miasto
NIP
Tokeny
Użytkownicy
BlueSky Logistics
Hiszpania
0
1
Trusted Partners Inc.
Francja
0
0
Dynamic Distributors
Stany Zjednoczone
0
0
ProSupply Solutions
Portugalia
0
0
Reliable Source Ltd.
Irlandia
0
0


Kategoria
Data zak. poprzedniego audytu 01-08-2023
Data zak. obecnego audytu 13-09-2023
Ogólna ocena poziomu dojrzałości Twojej organizacji
44%
45%
Polityka Bezpieczeństwa IT
100 %
60%
Budowanie świadomości
Rola Właściciela Biznesowego
Proces Zarządzania Ryzykiem w IT
Plan Ciągłości Działania
Zewnętrzni dostawcy usług IT
Dobre praktyki w obszarze bezpieczeństwa IT
Zarządzanie Incydentem
Zarządzanie uprawnieniami
Nadzór nad uprawnieniami
Zarządzanie zmianą & Software Development
Zarządzanie konfiguracją
Backup
Bezpieczeństwo Fizyczne
Pomieszczenia techniczne IT
Bezpieczeństwo serwerowni
Technologie w obszarze bezpieczeństwa IT
Bezpieczeństwo Infrastruktury LAN/WIFI
Bezpieczeństwo usług chmurowych
Bezpieczeństwo środowiska pracy użytkownika
12 %
12%
telescope
bkozlowski@sagenso.com
Owner
MENU
Strona Główna
Szablony Audytów
Audyty
Rekomendacje
Firmy
Audyty Anonimowe
Zarządzanie konfiguracją
Backup
Weryfikacja testów odtworzeniowych
Nie rozpoczęto
13-09-2023 08:09
W trakcie
03-10-2023 15:34
3
Do zatwierdzenia
03-10-2023 15:41
4
Zakończono
Okresowa weryfikacja jest niezbędna nie tylko z powodu potencjalnych pogorszeń w obszarze IT, które mogłyby wymagać działań naprawczych ale także ze względu na możliwą zmianę wymagań Organizacji np. w zakresie zdefiniowanych parametrów RTO i/lun RPO. Wskazany mechanizm kontrolny jest jednym z najważniejszych narzędzi do podtrzymania świadomości posiadanego stanu technologii i skuteczności procesowej w świetle aktualnych potrzeb biznesowych. Trzeba pamiętać, że ostateczną efektywność ocenia strona biznesowa (np. Właściciel Biznesowy) poprzez weryfikację czy odzyskane środowisko z kopii bezpieczeństwa jest zdatne do użytku, działa poprawnie i całość procesu zmieściła się w określonych wymaganiach (RTO i/lub RPO).
bkozlowski@sagenso.com zmienił status z W trakcie na Do zatwierdzenia
03-10-2023 15:41
bkozlowski@sagenso.com został przydzielony przez bkozlowski@sagenso.com
03-10-2023 15:37
bkozlowski@sagenso.com zmienił status z Nierozpoczęty na W trakcie
03-10-2023 15:34
bkozlowski@sagenso.com ustawił status na Nierozpoczęty
13-09-2023 08:09

Podsumowując:

Co Zarząd musi wiedzieć? Być świadomym odpowiedzialności.

Co Zarząd musi robić? Proaktywnie identyfikować i zarządzać zagrożeniami.

Co Zarząd może delegować? Wszystko poza nadzorem zarządczym.

Pierwszą rzecz zrobiliście sami. Wszystko inne możecie dostać w systemie **Telescope.**

Dziękuję za **uwagę!**

www.sagenso.com