PRAKTYCZNE BEZPIECZEŃSTWO ORGANIZACJI

OPARTE NA ISO 27001

BEZPIECZEŃSTWO INFORMACJI | TECHNOLOGIA I AI | LUDZIE I PROCESY | ZGODNOŚĆ I NORMY | BEZPIECZNA ORGANIZACJA

WERSJA BEZPŁATNA

Część 1

FUNDAMENTY

CYBERZAGROŻENIA

Jak chronić organizację w praktyce

DARIUSZ GOŁĘBIOWSKI

AUDYTOR WIODĄCY

Systemu Zarządzania Bezpieczeństwem Informacji

ISO 27001

poswojsku.pl

AKADEMIA BEZPIECZEŃSTWA GDDM

Pamiętaj proszę:

napracowałem się, uszanuj moje zaangażowanie i godziny pracy spędzone nad napisaniem i opracowaniem poradnika: ***Praktyczne bezpieczeństwo organizacji oparte na ISO 27001 Część 1 Fundamenty Wersja bezpłatna***. Poradnik powstał na bazie aktualnych przepisów oraz materiałów doradczo-szkoleniowych GDDM i poswojsku.pl, w tym szkoleń on-line dostępnych na portalu Akademia Bezpieczeństwa GDDM&poswojsku poswojsku.com.pl

Autor oraz Wydawnictwo poswojsku.pl

1. dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne, poprawne oraz rzetelne,
2. nie ponoszą żadnej odpowiedzialności za ewentualne szkody, które mogą wyniknąć z wykorzystania informacji zawartych w tej książce.

Wydawnictwo poswojsku.pl – kontakt:

www.poswojsku.pl, bok@poswojsku.pl

ul. Paprocka 86, 98-220 Zduńska Wola

ISBN: 978-83-68360-32-5

Proszę, czytaj tylko legalnie nabyte egzemplarze.

Od Autora Kilka słów o formach żeńskich i męskich

Wspaniała Czytelniczko - Drogi Czytelniku

Zależy mi, aby moje publikacje były przyjazne dla wszystkich osób. Jednocześnie staram się pisać w sposób prosty, naturalny i wygodny w czytaniu.

Dlatego w książce czasami używam form męskich, a czasami żeńskich. Wszystkie odnoszą się do każdej osoby czytającej tę publikację, niezależnie od płci, wieku, pochodzenia, stanowiska czy sposobu, w jaki sama siebie określa.

Nie stosuję konsekwentnie zapisów typu „czytelnik/czytelniczka", „nauczyciel/nauczycielka" itp., ponieważ utrudniają one płynność czytania.

Jeżeli ktoś zauważy, że liczba końcówek męskich nie zgadza się z liczbą końcówek żeńskich, z góry przepraszam. Nie jest to działanie zamierzone – po prostu jestem autorem książek ;), a nie księgowym końcówek językowych.

Życzę przyjemnej lektury wszystkim osobom czytającym tę książkę.

Praktyczne bezpieczeństwo organizacji oparte na ISO 27001 Część 1 Fundamenty - Wersja Bezpłatna

Poradnik powstał na bazie wewnętrznych materiałów szkoleniowych i doradczych właściciela firmy GDDM www.gddm.com.pl będącego certyfikowanym Audytorem Wiodącym Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001

✨

Spis treści

✨

WPROWADZENIE: DLACZEGO CZYTASZ TĘ KSIĄŻKĘ?

Chaos w Twoim biurze, informatycy biegną do serwerowni, prawnice nerwowo przeszukują akta dotyczące RODO, a Ty – osoba odpowiedzialna za bezpieczeństwo zastanawiasz się, czy ta sytuacja jest wynikiem wielomiesięcznego planowania napastnika, czy może - pracownik z działu marketingu kliknął w link z „darmową promocją na pizzę”?

Większość organizacji reaguje na takie sytuacje jak na klęskę przeznaczenia. Jednak jako ekspert bezpieczeństwa powiem właśnie Tobie coś, co może być nieprzyjemne dla niektórych:

To nie był wypadek. To był brak systemu. Kto zawalił? Dział IT? Czyżby? Tak uważasz?

Szefostwo powinno wiedzieć – za bezpieczeństwo nie odpowiada IT, tylko .. osoby zarządzające organizacją. Hmm, czyli być może .. Ty?

Właśnie powyższe idee oparte na metodologii ISO 27001 - przyświecają powstaniu tego poradnika.

Dlaczego napisałem tę książkę: Misja walki z mitem „bezpieczeństwa jako kosztu”

IT to „podatek”, który trzeba płacić. To czarna dziura w budżecie, w której pieniądze znikają na drogie urządzenia, których nikt nie rozumie i oprogramowanie spowalniające pracę pracowników. Taki jest mit!

Moim zadaniem jest zburzenie w.w. mitu.

Chcę pokazać, że bezpieczeństwo nie jest kosztem, tylko **fundamentem ciągłości biznesowej**.

Ta książka powstała z frustracji obserwowani organizacji, które kupują najdroższe „zamki” do drzwi, zostawiając jednocześnie okna otwarte na oścież. Piszę ją, aby przenieść ciężar dyskusji z „***ile wydamy na nowe narzędzia***” na „**jak zbudować odporną organizację**”.

Dla kogo jest ta książka?

Ten poradnik nie jest przeznaczony dla „osób technicznych”. Wręcz przeciwnie – jest stworzony dla każdego, kto ma udział w sukcesie organizacji:

- **Dla Kadry Zarządzającej (C-level):**

  Jeśli potrzebujesz zrozumieć ryzyko biznesowe, sposób na uniknięcie kar regulacyjnych i sposób na budowanie zaufania klientów poprzez bezpieczne procesy.

- **Dla Oficerów Bezpieczeństwa (CISO):**

  Jeśli szukasz konkretnej mapy drogowej, jak wdrożyć ISO 27001 bez „marnowania czasu” na biurokrację, która nie ma przełożenia na rzeczywiste zabezpieczenia.

- **Dla Menedżerów:**

  Jeśli chcesz wiedzieć, jak zabezpieczyć swoje zespoły, jakie procedury wprowadzić w pracy i jak nie być „wąskim gardłem” w procesie wdrażania zmian.

- **Dla Pracowników (szczególnie pragnących rozpocząć karierę w cyberbezpieczeństwie):**

  Jeśli chcesz zrozumieć, dlaczego Twoje hasło jest ważne, dlaczego procedury istnieją i jak stać się „żywą tarczą” organizacji, a nie jej najsłabszym ogniwem.

Serdecznie zapraszam na kolejne strony poradnika :)
o bezpieczeństwie organizacji,

Autor: Dariusz Gołębiowski

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001

strona domowa: www.gddm.com.pl

Krajobraz regulacyjny w UE: Dlaczego „teraz” jest kluczowe?

Jeśli myślisz, że „moim małym biznesem/organizacją nikt się nie zainteresuje”, to czas na małą korektę planów. Unia Europejska właśnie „podkręciła śrubę”.

Wchodzimy w erę **dyrektywy NIS2**. To już nie jest tylko opcjonalny „dobryton”. To zestaw twardych wymagań dotyczących odporności cyfrowej, raportowania incydentów i łańcucha dostaw dla szerokiego spektrum sektorów – od energetyki po administrację publiczną i medycynę.

Łącząc cyberbezpieczeństwo i RODO, stajemy przed faktem: **bezpieczeństwo staje się warunkiem koniecznym do prowadzenia działalności.** Niezapewnione bezpieczeństwo to ryzyko prawne, finansowe i wizerunkowe, które może wykluczyć organizację z rynku w jeden dzień.

Co to jest ISO 27001?

Jeśli usłyszałeś, że Twoja firma powinna

wdrażać ISO 27001 albo

SZBI oparte na metodologii ISO 27001,

a Twoją pierwszą myślą było: *„Czy to oznacza, że muszę kupić jeszcze więcej drogich programów i zatrudnić armię informatyków?”* – mam dla Ciebie dobrą wiadomość. **Nie.**

Najprostsza definicja brzmi:

ISO 27001 to światowy standard zarządzania bezpieczeństwem informacji.

Ale co to oznacza w praktyce, jeśli nie jesteś ekspertem? Pozwól, że użyję trzech prostych porównań.

1. ISO 27001 to „Plan Budowy Bezpiecznego Domu”

Wyobraź sobie, że budujesz dom. Możesz kupić najdroższe drzwi, ale jeśli nie zaplanowałaś, gdzie wpuścisz gości, a okna zostawisz na parterze, drzwi nic nie znaczą.

ISO 27001 nie mówi Ci, jaką konkretnie markę zamka masz kupić. Zamiast tego daje Tobie i Twojej organizacji **kompletny plan**:

- Gdzie masz najcenniejsze rzeczy (pieniądze, dokumenty)?
- Kto ma do nich klucz i dlaczego?
- Co zrobisz, jeśli ktoś spróbuje włamać się w nocy?
- Jak często sprawdzasz, czy zamki nadal działają?

2. ISO 27001 to „System Zarządzania” (a nie - jednorazowa akcja)

Wielu ludzi myśli, że bezpieczeństwo to „instalacja antywirusa”albo nie wyłączanie firewall. ISO 27001 mówi:

„Nie, bezpieczeństwo to **system**”.

To różnica między kupieniem gaśnicy (jednorazowe działanie), a posiadaniem kompleksowego systemu przeciwpożarowego, który obejmuje:

- **Szkolenie** ludzi, jak nie wywołać pożaru.
- **Procedury** ewakuacyjne.
- **Regularne przeglądy** instalacji.
- **Analizę ryzyka** (czy np. kuchnia nie jest zbyt blisko magazynu paliw?).

W języku ISO nazywamy to **SZBI (System Zarządzania Bezpieczeństwem Informacji)**. To „instrukcja obsługi" Twojej firmy, która pilnuje, by bezpieczeństwo było stałym elementem codziennej pracy, a nie projektem, który robi się raz w roku.

3. ISO 27001 to „Certyfikat Zaufania”

Na rynku globalnym ISO 27001 działa jak „paszport” dla Twojej firmy. Kiedy pokazujesz klientowi certyfikat ISO 27001, mówisz mu:

> *„Nie obiecuję Tobie magicznie, że nigdy nas nie zhakują (bo przy obecnym poziomie technologii - nikt nie może tego zagwarantować).*
>
> *Ale obiecuję Tobie„ że mamy profesjonalny system, który identyfikuje zagrożenia, chroni Twoje dane zgodnie z najlepszymi światowymi standardami i potrafi zareagować, gdy coś pójdzie nie tak”.*

ISO 27001 to system mający zapewnić tzw. “ciągłość działania”.

Czym ISO 27001 NIE jest?

(Najczęstsze mity)

- **Nie jest listą „technicznych zabawek”:**

  To nie jest lista kontrolna „czy masz firewall”. To lista pytań o zarządzanie: „czy wiesz, co robisz, gdy firewall zawiedzie?”.

- **Nie jest „papierologią dla samej papierologii”:**

  Jeśli dokumenty nie mają przełożenia na to, jak pracują ludzie i jak działają systemy, to wdrożenie ISO jest błędne, a może nawet - zbędne.

- **Nie jest celem samym w sobie:**

  Celem ISO nie jest zdobycie certyfikatu “na ścianę”. Celem jest **odporność organizacji** na m.in.: ataki, wycieki danych i błędy ludzkie.

ISO 27001 to przejście z trybu

„Mamy nadzieję, że nas nie zhakują”

do trybu

„Wiemy, co może pójść nie tak, i wiemy dokładnie, jak na to zareagować”.

Metodologia ISO 27001 - to przejście od chaosu do uporządkowanego procesu,

który chroni

Twoje pieniądze,

Twoich klientów,

Twoją reputację.

ROZDZIAŁ 1: DLACZEGO ORGANIZACJE WPADAJĄ W KŁOPOTY

Plan Rozdziału

1. **Wstęp: Anatomia porażki** – Krótkie wprowadzenie w cyberbezpieczeństwo.
2. **Scenariusze z życia wzięte (Autopsje):**
    1. *Scenariusz A: Paraliż urzędowy* – Jak jeden klik może zatrzymać usługi publiczne.
    2. *Scenariusz B: „Wysyłka do wszystkich”* – Koszty utraty zaufania i kary regulacyjne.
    3. *Scenariusz C: „Ups, nie chciałem”* – Przypadkowe usunięcie danych jako cichy zabójca ciągłości.
3. **Technologia vs. Organizacja** – Dlaczego lepsze zabezpieczenia nie rozwiązują problemu braku procesów.
4. **Podsumowanie rozdziału – fundament serii.**

Wyobraź sobie poniedziałek rano. Kawa jest jeszcze ciepła, pracownicy siadają do biurek, a Ty – jako lider organizacji – planujesz ambitny tydzień. Nagle telefon dzwoni po raz dziesiąty w ciągu minuty. Pracownicy nie mogą się zalogować do systemu, klienci zaczynają dzwonić z pretensjami, a Twój dział IT właśnie wysłał wiadomość:

„Mamy problem. Bardzo duży problem".

Większość organizacji traktuje cyberbezpieczeństwo jako rodzaj „ubezpieczenia" – coś, co kupujesz raz, płacisz za to składkę i liczysz na to, że nic się nie stanie. Prawda jest jednak brutalna:

Bezpieczeństwo (i/lub cyber) nie jest produktem, który można kupić i postawić na półce. To stan Twojej organizacji.

Aby zrozumieć, dlaczego wciąż wpadamy w kłopoty, przyjrzyjmy się pięciu klasycznym scenariuszom, które zdarzają się w częściej, niż chciałabyś przyznać.

Scenariusz A: Paraliż urzędowy (Ransomware)

Przykład:

Urząd w małym mieście, który nagle „przestał istnieć” dla mieszkańców.

W jednym z przypadków (a jest ich co najmniej kilka w roku) - urząd gminy został sparaliżowany przez ransomware. Nagle komputery zaczęły wyświetlać żądania okupu, a dostęp do rejestrów, dokumentacji mieszkańców i systemu płatności został zablokowany. Co się wydarzyło? Urząd nie mógł wystawiać decyzji, nie mógł przyjmować wniosków, a mieszkańcy stali w kolejkach, nie wiedząc, dlaczego system „nie działa”.

I wcale nie to co powyżej opisałem mogło być najgorsze. Bo zanim hakerka nieetyczna założy ransomware – najpierw zwykle kradnie dane.

A Ty jako mieszkaniec, którego dane są dostępne w Darknecie – jak się poczujesz?

Dlaczego to się stało?

Technologia (firewall, antywirus) mogła działać poprawnie, ale może brakowało:

- skutecznych i regularnych szkoleń dla całego personelu - ktoś kliknął w groźny link, bo ze względów oszczędnościowych oraz praktycznych (tak się to często tłumaczy) – personel uczestniczył jedynie w mało efektywnych szkoleniach elearning,
- procesu regularnego tworzenia kopii zapasowych w wydzielonym miejscu,
- procedury szybkiego odzyskiwania danych po ataku,
- .. i wielu innych braków ;(

Scenariusz B: „Wysyłka do wszystkich” (Wyciek danych)

Przykład:

Firma e-commerce wysyła bazy danych 50 000 klientów do… niewłaściwego odbiorcy.

Pracownik działu marketingu, chcąc szybko przygotować kampanię, kopiuje plik Excela z danymi osobowymi i numerami telefonów klientów. Przez pomyłkę przesyła go do zewnętrznego kontrahenta lub wrzuca na publiczną chmurę, do której każdy ma dostęp.

Efekt? Gigantyczny kryzys wizerunkowy, powiadomienia od Urzędu Ochrony Danych Osobowych i konieczność wypłacenia odszkodowań.

Dlaczego to się stało?

W tym przypadku problemem nie był brak technologii. Tu brakowało **procesu** bezpiecznego przesyłania danych oraz świadomości pracownika, czym jest „informacja wrażliwa".

A powody – kilka wymieniłem już powyżej, a o innych jeszcze będzie czas, aby opowiedzieć w tej serii poradników.

Scenariusz C: „Ups, nie chciałem” (Błąd ludzki)

Przykład:

„Przecież tylko chciałem zrobić porządki na pulpicie”.

Administrator bazy danych, chcąc zwolnić miejsce na dysku, usuwa folder, który wydawał mu się nieużywany.

Okazuje się, że był to folder z archiwalnymi umowami z ostatnich 5 lat. Cała praca zespołu, która trwała miesiące, znika w sekundę.

Dlaczego to się stało?

Bo w organizacji nie istniała zasada „nadzoru nad zmianami” ani jasna instrukcja, co można usuwać, a co jest krytycznym aktywem.

Technologia vs. Organizacja

Wielu dyrektorów pyta mnie:

„Jaką technologię mam kupić, żeby to nie spotkało mojej organizacji?”

Moja odpowiedź brzmi:

Technologia jest tylko narzędziem,

a organizacja jest architekturą.

Możesz kupić najdroższy firewall świata, ale jeśli pracownicy nie wiedzą, jak rozpoznawać podejrzane maile, firewall nie pomoże. Możesz kupić najnowocześniejszy system backupu, ale jeśli nikt nie sprawdzi raz w miesiącu, czy kopie faktycznie działają, Twój backup jest tylko drogo płacącym złudzeniem bezpieczeństwa.

Bezpieczeństwa nie da się kupić. Bezpieczeństwo buduje się poprzez procesy, kulturę i jasne zasady.

Podsumowanie rozdziału

W większości przypadków problemem organizacji nie był brak technologii, ale brak organizacji. To jest fundament całej serii:

zanim zainwestujesz choćby złotówkę w nowe oprogramowanie,

musisz najpierw uporządkować zasady gry w swojej organizacji.

Bez porządku technologia jest tylko drogim gadżetem. Z porządkiem - staje się fundamentem odporności.

ISO 27001 wymaga **dokumentowania wiedzy** nie po to, by tworzyć „bibliotekę kurzu", ale by **organizacja była niezależna od** kaprysów czy zdrowia jednej osoby. To **wzmacnia argument o ciągłości biznesowej**.

ROZDZIAŁ 2: CZYM NAPRAWDĘ JEST BEZPIECZEŃSTWO ORGANIZACJI

Plan Rozdziału

1. **Wstęp: Pułapka „Zamkniętych Drzwi”** – Rozróżnienie między bezpieczeństwem technicznym a bezpieczeństwem organizacji.
2. **Nowa definicja: Bezpieczeństwo jako zdolność do działania** – „Przeżycie ataku” to za mało, „nadal świadczyć usługi” - cel nadrzędny.
3. **Piramida Wartości Bezpieczeństwa:**
    A) **Ciągłość działania**
    B) **Odporność**
    C) **Zgodność**
    D) **Klasyczna Triada CIA:**
4. **Przykład z życia: Szpital vs. Sklep internetowy**
5. **Podsumowanie rozdziału.**

Jeśli zapytasz przeciętnego pracownika, czym jest ***cyberbezpieczeństwo***, większość odpowie: „to te wszystkie hasła, antywirusy i pilnowanie, żeby nikt nie włamał się na komputer”. Jeśli zapytasz menedżera średniego szczebla, może powie: „to te wszystkie zakazy, które utrudniają mi szybkie wykonanie pracy”. A jeśli zapytasz prezesa, może powie: „***to coś, za co musimy płacić, żeby uniknąć kary od urzędu***”.

Wszystkie te odpowiedzi są częściowo prawdziwe, ale żadna nie oddaje istoty bezpieczeństwa organizacji.

Wiele firm popełnia błąd, myśląc, że bezpieczeństwo to zestaw „zamków” na drzwiach cyfrowego biurowca. Ale co z tego, że drzwi są solidne, jeśli w środku nie ma wody, prądu ani pracowników zdolnych do pracy? **Bezpieczeństwo organizacji to nie jest stan „niedostępności dla innych”. To zdolność organizacji do działania w założonych warunkach, nawet gdy ktoś próbuje tę zdolność zakłócić.**

Bezpieczeństwo jako zdolność do działania

Wyobraź sobie szpital. Jeśli systemy informatyczne w szpitalu padną, problemem nie jest tylko to, że pielęgniarki nie mogą wpisać danych do komputera. Problemem jest to, że lekarz nie może sprawdzić grupy krwi pacjenta, a apteka nie wie, jaką dawkę leku podać.

W tym kontekście bezpieczeństwo, to nie „hasło do systemu". **Bezpieczeństwo** to **zdolność do ratowania życia w każdych warunkach**. To jest nadrzędny cel, a technologia jest jedynie narzędziem, które tę zdolność wspiera.

W bezpieczeństwie organizacji musimy patrzeć na cztery filary, które układają się w hierarchię ważności dla biznesu.

Przykład z życia: Szpital vs. Sklep internetowy

Zrozumienie tych różnic jest kluczowe dla każdego lidera. Także dla Ciebie Pani Prezes ;).

Wyobraźmy sobie dwa różne biznesy:

1. **Szpital:**

   Tutaj priorytetem jest **Dostępność i Ciągłość**. Jeśli system padnie, życie ludzkie jest zagrożone. Tutaj bezpieczeństwo oznacza, że systemy muszą działać 24/7, nawet jeśli oznacza to droższe redundantne serwery.
2. **Sklep internetowy:**

   Tutaj priorytetem może być **Poufność**. Jeśli sklep padnie na godzinę, straci sprzedaż. Jeśli jednak wycieknią numery kart kredytowych 100 tysięcy klientów, sklep może zbankrutować w jeden dzień przez kary i utratę zaufania.

Wniosek?

Bezpieczeństwo nie jest „jednakowe” dla każdego. Musisz wiedzieć, co dla Twojej organizacji jest krytyczne. Czy jest to dla przykładu:

- szybki powrót do pracy (odporność)?
- ochrona tajemnic handlowych (poufność)?

To Ty - jako strateg Twojej organizacji - musisz podejmować decyzje w sprawie istniejących priorytetów. Twoim zadaniem będzie takie ich wypośrodkowanie, aby zoptymalizować korzyści dla Twojej organizacji.

Podsumowanie rozdziału

Bezpieczeństwo organizacji to:

- nie jest zestaw najnowszych (ani starszych) narzędzi informatycznych.

Bezpieczeństwo organizacji to:

- ***strategiczna zdolność do ciągłego, efektywnego działania,***
- ***odporność na zakłócenia,***
- ***zgodność z prawem,***
- ***fundament, na którym organizacja buduje zaufanie i ciągłość swojej działalności.***

A Ty szefie, zanim zaakceptujesz konkretne oprogramowanie, musisz odpowiedzieć na pytanie: ***co w mojej organizacji jest krytyczne dla przeżycia***?

Pozwól proszę, że na chwilkę Ciebie oderwę od tej pasjonującej lektury :)

Informacja od autora: Autor książki świadczy również usługi szkoleniowe, doradcze i audytowe związane z tematyką bezpieczeństwa informacji, cyberbezpieczeństwa i ISO 27001. Informacje o tych usługach zostały zamieszczone w celach informacyjnych dla osób zainteresowanych dalszym rozwojem w omawianych obszarach.

Być może czytasz ten poradnik, bo potrzebujesz wsparcia we wdrażaniu bezpieczeństwa?

Przeczytanie książki to doskonały pierwszy krok. W wielu organizacjach pojawia się jednak pytanie:

„Co dalej?"

Jeżeli chcesz:

- uporządkować bezpieczeństwo informacji,
- przygotować organizację do wymagań ISO 27001, NIS2 lub uKSC,

mogę pomóc Tobie oraz Twojej organizacji przejść tę drogę szybciej, spokojniej i z mniejszą liczbą błędów.

AUDYTY WEWNĘTRZNE ISO 27001

Przeprowadzam audyty wewnętrzne Systemów Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami normy ISO/IEC 27001.

Podczas audytu pomagam odpowiedzieć między innymi na pytania:

✓ Czy nasze działania są zgodne z wymaganiami normy?

✓ Czy dokumentacja wspiera organizację, czy tylko istnieje „na papierze”?

✓ Czy analiza ryzyka jest aktualna i użyteczna?

✓ Czy kierownictwo posiada informacje potrzebne do podejmowania decyzji?

✓ Jakie obszary wymagają poprawy przed audytem certyfikującym?

Celem audytu nie jest szukanie winnych. Celem jest wskazanie obszarów do doskonalenia i zwiększenie poziomu bezpieczeństwa organizacji.

PRZYGOTOWANIE DO AUDYTÓW ISO 27001

Wiele organizacji obawia się pierwszego audytu certyfikującego.

Niepotrzebnie.

Pomagam przygotować organizacje do procesu certyfikacji poprzez:

✓ przegląd istniejącego SZBI,

✓ analizę zgodności z wymaganiami normy,

✓ identyfikację braków i obszarów ryzyka,

✓ wsparcie w przygotowaniu dokumentacji,

✓ przygotowanie kierownictwa i pracowników do rozmów audytowych.

Moim celem jest nie tylko pomoc w uzyskaniu certyfikatu, ale przede wszystkim stworzenie systemu, który realnie wspiera organizację.

SZKOLENIA Z BEZPIECZEŃSTWA INFORMACJI, CYBERBEZPIECZEŃSTWA, SZBI oraz RODO

Prowadzę szkolenia stacjonarne oraz online dla:

✓ firm,

✓ szkół,

✓ jednostek samorządu terytorialnego,

✓ instytucji publicznych,

✓ organizacji pozarządowych.

Najczęściej realizowane tematy:

- Bezpieczeństwo informacji w organizacji
- Cyberzagrożenia i cyberhigiena
- NIS2 w praktyce
- uKSC (Krajowy System Cyberbezpieczeństwa)
- SZBI i ISO 27001
- Analiza ryzyka
- Odpowiedzialność kierownictwa
- Bezpieczne wykorzystanie AI w organizacji

Szkolenia prowadzone są prostym, praktycznym językiem, bez nadmiaru teorii i niezrozumiałego żargonu.

Dlaczego warto?

Jestem certyfikowanym Audytorem Wiodącym Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001 i od lat wspieram organizacje w budowaniu praktycznego podejścia do bezpieczeństwa informacji, zarządzania ryzykiem oraz zgodności z wymaganiami prawa i norm.

Moim celem nie jest tworzenie kolejnych segregatorów dokumentów.

Moim celem jest pomoc organizacjom w budowaniu bezpieczeństwa, które działa w praktyce.

🌐 www.gddm.com.pl

📧 bok@poswojsku.pl

Praktyczne bezpieczeństwo Twojej organizacji.

ROZDZIAŁ 3: Informacja jest aktywem - Myślenie ISO

Plan Rozdziału

1. **Wstęp: Koniec z „plikami na dysku”** – Przełamanie myślenia, że bezpieczeństwo dotyczy tylko komputerów.
2. **Zmiana paradygmatu: Informacja jako paliwo biznesowe**

   Dlaczego dane są nową walutą i dlaczego ich utrata jest jak utrata kapitału.
3. **Katalog Aktywów – Przykłady sektorowe:**

   Edukacja, Biznes, Sektor Publiczny.
4. **Koncepcja Właścicielstwa Aktywów (Asset Ownership)**

   Najważniejszy punkt ISO: Dlaczego informatyk nie jest właścicielem Twoich danych?

Jeśli chcesz zacząć myśleć jak ekspertka od bezpieczeństwa - zgodnie ze standardem ISO 27001, musisz dokonać co najmniej jednej, fundamentalnej zmiany w sposobie myślenia. Musisz przestać myśleć o „bezpieczeństwie komputerów", a zacząć myśleć o **„bezpieczeństwie informacji"**. Podkreślę dla tych, którzy są przesiąknięci tzw. RODO:

nie chodzi o bezpieczeństwo danych, tylko o bezpieczeństwo informacji.

A to wielka, bardzo wielka różnica.

Wielu menedżerów popełnia błąd, zakładając, że jeśli kupią:

- lepsze komputery, laptopy, serwery,
- bardziej nowoczesne oprogramowanie,
- szybszy internet,

to ich organizacja będzie zupełnie bezpieczna.

To tak, jakbyś kupiła najbardziej nowoczesny sejf, ale zostawiła w nim otwarte drzwi do budynku. W firmie tymi otwartymi drzwiami może być personel – słabo przeszkolony z cyberhigieny i niedostatecznie uświadomiony z możliwości jakie mają cyberprzestępcy (choćby co do wykorzystania tzw. Phishingu).

Bezpieczeństwo w modelu ISO 27001 zaczyna się od zrozumienia, że **informacja jest aktywem**. Jest tym, co budujesz, co sprzedajesz i co chroni Twoją pozycję na rynku.

Zmiana paradygmatu: Informacja jako paliwo biznesowe

W dzisiejszej gospodarce informacja jest jak paliwo. Może napędzać Twój biznes (bazy danych klientów, analizy rynkowe, autorskie algorytmy), ale może też stać się przyczyną katastrofy, jeśli „wycieknie" lub zostanie „zmieniona".

Gdy informacja staje się aktywem, zmienia się sposób, w jaki o nią dbamy. Nie pytamy już tylko:

„Czy ten serwer działa?", ale pytamy:

„Jakie informacje znajdują się na tym serwerze i co się stanie, jeśli ktoś je ukradnie, zmieni lub jeśli przestaniemy mieć do nich dostęp?".

Katalog Aktywów – Przykłady sektorowe

Aby lepiej zrozumieć opisywane zagadnienia, przyjrzyjmy się, jak różne organizacje definiują swoje najważniejsze aktywa. Każda z nich ma inny „szczyt priorytetów", który musi chronić:

- **Szkoła / Placówka Oświatowa:**

  Dla dyrektora szkoły „aktywami" nie są tylko tablety w klasach. To przede wszystkim: **dzienniki elektroniczne, dokumentacja uczniów, wyniki egzaminów oraz dane osobowe rodziców oraz – równie ważne – dane osobowe personelu**.

  Jeśli te dane wyciekną, szkoła traci zaufanie społeczne. Jeśli zostaną usunięte, proces dydaktyczny staje się niemożliwy.

- **Firma / Startup / Korporacja:**

  Tutaj aktywa mają często bezpośrednią wartość rynkową. To **bazy danych klientów, umowy handlowe, kody źródłowe oprogramowania, strategie marketingowe oraz tajemnice handlowe**. Wyciek bazy klientów do konkurencji to nie tylko problem techniczny – to bezpośredni cios w portfel firmy i jej przewagę konkurencyjną.

- **Urząd / Jednostka Administracji Publicznej:**

  W sektorze publicznym aktywa to fundament demokracji i porządku prawnego. Są to **dane mieszkańców, akta stanu cywilnego, decyzje administracyjne, plany zagospodarowania przestrzennego**. Tutaj priorytetem jest integralność (pewność, że dokument jest prawdziwy) i dostępność (obywatel musi móc uzyskać usługę).

Koncepcja Właścicielstwa Aktywów: Kluczowy punkt ISO

Tutaj dochodzimy do punktu, w którym większość organizacji ma wielki problem ze zrozumieniem istoty rzeczy. W standardzie ISO 27001 istnieje kluczowa zasada:

Każdemu aktywu musi być przypisany Właściciel.

I tutaj pojawia się pułapka. Wielu prezesów myśli, że właścicielem danych jest dział IT, bo to oni trzymają je na serwerach. **To błąd, wielki strategiczny błąd, który prowadzi do nieefektywnego wdrożenia SZBI.**

Klasyfikacja informacji – Oddzielanie „szumu” od „diamentów”

Skoro wiemy już, że informacja jest aktywem, musimy nauczyć się je sortować. Nie wszystkie informacje są sobie równe. Jeśli będziesz próbowała chronić wszystko z taką samą siłą, przepłacisz i utrudnisz życie pracownicom.

Metodologia ISO 27001 sugeruje myślenie o klasyfikacji.

Możemy podzielić informacje na - dla przykładu - trzy poziomy:

1. **Publiczne:**

   Informacje, które mogą być dostępne dla każdego (np. oferta w Internecie).

2. **Wewnętrzne:**

   Informacje dla pracowników, które nie są tajne, ale nie powinny być publiczne (np. komunikacja wewnętrzna, ogłoszenia o pracę).

3. **Poufne / Tajne:**

   Informacje, których wyciek powoduje realne straty (np. dane medyczne, numery kont, strategie fuzji).

Pozwól, że dodam bardzo istotne stwierdzenie: “każda organizacja może zdefiniować własną skalę”. Mówię o tym, abyście drogi Czytelniku/ Wspaniała Czytelniczko nie czuli się ograniczeni tylko do tych trzech wyżej wymienionych.

ROZDZIAŁ 4: RYZYKO – NAJWAŻNIEJSZE SŁOWO W BEZPIECZEŃSTWIE

Plan Rozdziału

1. **Wstęp: Demistyfikacja „Strachu”**
2. **Co to właściwie jest ryzyko? (Definicja dla ludzkich głów)**
3. **Iluzja 100% bezpieczeństwa**
4. **Skutki, które bolą (Typologia skutków):**
5. **Apetyt na ryzyko – jak podejmować rozsądne decyzje?**
6. **Zarządzanie zamiast paniki**
7. **Podsumowanie rozdziału.**

Jeśli otworzysz podręcznik do zarządzania ryzykiem, prawdopodobnie znajdziesz tam setki stron skomplikowanych wzorów matematycznych, tabele z dziesięcioma cyframi po przecinku i wykresy, które wyglądają, jakby projektował je ktoś po co najmniej habilitacji czy może raczej kilku kawach w ciągu jednej nocy.

Dobra wiadomość jest taka:

Dla lidera organizacji te wzory nie są najważniejsze.

W świecie cyberbezpieczeństwa ryzyko nie jest problemem matematycznym. Ryzyko jest **decyzją biznesową**. Jeśli zrozumiesz to teraz, unikniesz największej pułapki, w jaką wpadają firmy: inwestowania ogromnych sum w zabezpieczenia przed zagrożeniami, które mają znikome prawdopodobieństwo wystąpienia, przy jednoczesnym ignorowaniu realnych zagrożeń, które mogą zniszczyć firmę w jeden dzień.

Co to właściwie jest ryzyko? (Definicja zrozumiała dla większości ludzi)

W najprostszych słowach, ryzyko to odpowiedź na dwa pytania:

1. **Co może się stać?** (Zagrożenie)
2. **Jak bardzo nas to zaboli, jeśli to się stanie?** (Skutek)

W profesjonalnym świecie mnożymy te dwa elementy:

Ryzyko = Prawdopodobieństwo × Skutek

Przykład:

- **Zagrożenie A:**

  Atak hakerski na Twój system płatności.
  Prawdopodobieństwo: Średnie.

Skutek: Bardzo wysoki (utrata pieniędzy, kary, wizerunek).

Ryzyko: Wysokie.

- **Zagrożenie B:**

  Pracownik przypadkowo wyśle maila do niewłaściwej osoby.

  Prawdopodobieństwo: Bardzo wysokie.

  Skutek: Niski (mała strata danych).

  Ryzyko: Średnie.

Zrozumienie tej różnicy pozwala Tobie przestać „walczyć ze wszystkim” i zacząć „zarządzać tym, co jest naprawdę ważne”.

Iluzja 100% bezpieczeństwa

Tutaj pojawia się brutalna prawda:

Nie da się wyeliminować wszystkich zagrożeń.

Jeśli ktoś powie Ci, że oferuje rozwiązanie gwarantujące 100% bezpieczeństwa, albo kłamie, albo nie rozumie, jak działa świat. Każda technologia ma luki, każdy człowiek może się pomylić, a każdy haker znajdzie nową drogę.

Dążenie do 100% bezpieczeństwa jest nie tylko niemożliwe, ale też bardzo szkodliwe dla rozwoju biznesu. Dlaczego?

Bo

im bardziej chcesz być bezpieczny, tym bardziej ograniczasz swoją zdolność do działania.

Jeśli zamkniesz wszystkie drzwi, wyłączysz internet, zablokujesz dostęp do plików i wymagasz pięciu poziomów autoryzacji do wypicia kawy – Twoja firma przestanie działać. Ale będzie bardzo bezpieczna, a nawet super cyberbezpieczna.

Tymczasem:

bezpieczeństwo to sztuka kompromisu.

Chodzi o to, by bezpieczeństwo było

wystarczające, by chronić to, co ważne,

ale jednocześnie

na tyle elastyczne, by nie paraliżować pracy personelu.

Skutki, które bolą (Typologia skutków)

Kiedy analizujesz ryzyko w organizacji, nie patrz tylko na tzw, „hakerów". Patrz na to, jak atak wpłynie na Twoje cele biznesowe.

Skutki dzielimy na cztery kategorie:

1. **Finansowe:**

   Bezpośrednie straty (okupy, kary administracyjne, koszty naprawy systemów, utracone przychody).

2. **Operacyjne:**

   Paraliż firmy. Czy Twoi pracownicy mogą pracować? Czy klienci mogą korzystać z Twoich usług? To jest „koszt przestoju".

3. **Wizerunkowe:**

   Utrata zaufania. Raz stracone zaufanie klientów jest najtrudniejszą rzeczą do odzyskania. W dobie mediów społecznościowych informacja o wycieku danych rozchodzi się szybciej niż jakikolwiek wirus.

4. **Prawne:**

   Konsekwencje wynikające z braku zgodności z przepisami (np. NIS2 w UE, które nakłada surowe obowiązki na sektory kluczowe).

Podsumowanie rozdziału

Ryzyko to nie jest wróg, którego należy całkowicie pokonać.

Ryzyko to element prowadzenia każdego biznesu.

Twoim zadaniem jako liderki nie jest eliminowanie ryzyka, bo to po prostu jest niemożliwe.

Twoim zadaniem jest **zarządzanie ryzykiem** w sposób, który pozwala Twojej organizacji bezpiecznie realizować swoje cele.

Zmień strach Twoj I organizacji - na analizę, a analizę na świadomą decyzję.

ROZDZIAŁ 5: LUDZIE, PROCESY I TECHNOLOGIA (ZŁOTY TRÓJKĄT)

Plan Rozdziału

1. **Wstęp: Pułapka „Magicznego Pudełka”**
2. **Koncepcja Złotego Trójkąta**
3. **Podsumowanie rozdziału.**

Wstęp: Pułapka „Magicznego Pudełka”

Wyobraź sobie firmę, która po serii artykułów o cyberatakach postanawia działać „natychmiast”. Zarząd przeznacza znaczną kwotę na zakup:

najnowocześniejszego, „nie do pokonania” systemu detekcji zagrożeń (EDR) oraz

najdroższego na rynku firewalla.

Kupują technologię, która w folderach reklamowych producenta wygląda jak tarcza niezniszczalnego superbohatera.

Niestety, miesiąc później firma zostaje sparaliżowana przez ransomware. Wszystkie systemy zablokowane.

Dlaczego? Co się stało?

Pomimo posiadania technologii:

- najnowszej z najnowszych,
- najdroższej z najdroższych,

pracownicy wciąż używali wspólnych haseł do wszystkich systemów, a polityka wydawania uprawnień do baz danych nie istniała (każdy miał dostęp do wszystkiego, „bo tak było wygodniej").

Wniosek jest brutalny:

Kupowanie oprogramowania to tylko połowa walki, a często nawet nie połowa. Technologia bez odpowiednich procesów i świadomych ludzi jest jak najdroższy zamek antywłamaniowy zamontowany na drzwiach, które zostawiono otwarte na oścież. To nie jest strategia bezpieczeństwa; to jedynie „kupowanie poczucia bezpieczeństwa".

Koncepcja Złotego Trójkąta

W świecie profesjonalnego cyberbezpieczeństwa, opartego na standardach takich jak ISO 27001, mówimy o **Złotym Trójkącie**.

Aby organizacja była naprawdę bezpieczna, trzy filary muszą współgrać w idealnej równowadze:

1. **Ludzie**

   Kto to robi i czy świadomie rozumie - dlaczego?

2. **Procesy**

   Jak to robimy – procesowo czy papierkowo? I czy jest to powtarzalne?

3. **Technologia**

   Jakie narzędzia nam w tym pomagają? Najnowocześniejsze czy najlepiej dopasowane do naszych potrzeb?

Jeśli jeden z tych filarów jest słabszy od pozostałych, cały trójkąt się rozapada:

- Jeśli masz ***świetnych ludzi i procesy***, ale słabą technologię – organizacja będzie pracowała zbyt wolno i narażona będzie na różnorodne zewnętrzne ataki.
- Jeśli masz ***technologię i procesy***, ale nie masz przeszkolonych ludzi – Twoi pracownicy rozwalą system od środka, bo nie rozumieją jego celu i nie posiadają odpowiedniej świadomości co do zagrożeń.
- Jeśli masz ***ludzi i technologię***, ale brak procesów – Twoje bezpieczeństwo będzie zależeć od humoru i pamięci konkretnych osób, a przyznasz zapewne, że to może być drogą do pięknej katastrofy.

Podsumowanie rozdziału

Bezpieczeństwo organizacji nie jest wynikiem zakupu jednego konkretnego programu, a nawet całego zestawu najlepszego z najlepszych – systemu IT.

Bezpieczeństwo jest wynikiem świadomej budowy ekosystemu, w którym:

- **Ludzie** doskonale wiedzą, co robią i dlaczego.
- **Procesy** jasno definiują, jak mają to robić.
- **Technologia** umożliwia im robić to szybko i skutecznie.

Jeśli czujesz, że w Twojej organizacji jeden z tych filarów kuleje – ***przestań kupować nowe narzędzia. Zacznij naprawiać fundamenty***. Tylko wtedy ***Twój „Trójkąt" stanie się stabilną konstrukcją***, zdolną przetrwać sztorm w cyfrowym świecie.

ROZDZIAŁ 6: CZYM JEST ISO 27001 - w wielkim skrócie

Plan Rozdziału

1. **Wprowadzenie: Mit „Biurokratycznego Potwora”**
2. **ISO jako mapa, a nie cel podróży**
3. **Serce normy: Podejście oparte na ryzyku (Risk-based approach)**
4. **ISO 27001 jako „szablon porządku”**
5. **Podsumowanie rozdziału: Krótka lista „Dlaczego to robimy?”**

Jeśli słyszysz skrót ***„wdrażamy ISO 27001”*** w rozmowach biurowych, Twoja pierwsza reakcja może być jedna z dwóch:

- poczujesz nagły przypływ dumy, że Twoja firma jest „nowoczesna”,
- co bardziej prawdopodobne – poczujesz lekki ból głowy na myśl o setkach stron dokumentacji i biurokracji, która ma nadejść.

Wiele organizacji traktuje ISO 27001 jak „biurokratycznego potwora” – gigantyczną machinę papierową, której celem jest - certyfikat, by powiesić go na ścianie i użyć jako ozdoby w ofertach handlowych.

Prawda jest jednak zupełnie inna. ISO 27001 nie jest celem samym w sobie. To potężne narzędzie, które ma sprawić, że Twoja organizacja przestanie „ślepo” walczyć z cyberzagrożeniami, a zacznie nimi świadomie zarządzać.

ISO jako mapa, a nie cel podróży

Wyobraź sobie, że planujesz wyprawę przez góry. Możesz:

- kupić nowoczesny samochód z pancernym podwoziem - jego odpowiednik w organizacji to najdroższe oprogramowanie antywirusowe,
- posiadać zapasy jedzenia - odpowiednik w organizacji to najwyższej klasy firewall.

Jeśli jednak wyjedziesz w trasę bez mapy, możesz wjechać prosto w przepaść, bo nie wiedziałaś, gdzie jest objazd, a gdzie most jest zniszczony.

ISO 27001 jest właśnie odpowiednikiem mapy, dzięki której nie wpadniesz w przepaść.

ISO 27001:

- Mówi Twojej organizacji, gdzie na drodze czekają najpoważniejsze zagrożenia (analiza ryzyka).
- Pokazuje, jakie zasady bezpieczeństwa musisz przestrzegać, aby dotrzeć do celu (polityki i procedury).
- Podpowiada, jak reagować, gdy na drodze zdarzy się awaria (zarządzanie incydentami).

Ważna uwaga:

Sama mapa nie prowadzi samochodu. Organizacja może mieć certyfikat ISO 27001 i wciąż być narażona na ataki, jeśli Twój zespół nie będzie przestrzegał wyznaczonych zasad. Certyfikat to dowód na to, że *masz plan*. Ale to Ty i Twoi pracownicy musicie ten plan realizować każdego dnia.

Serce normy: Podejście oparte na ryzyku (Risk-based approach)

To jest najważniejszy punkt, który odróżnia profesjonalne bezpieczeństwo od „bezpieczeństwa na oślep”. Wiele firm popełnia błąd: „wszystko jest ważne”.

Próbują zabezpieczyć: każdy kabel, każdy e-mail i każdy folder z taką samą intensywnością.

Efekt?

Przeładowanie budżetu, frustracja pracowników i ogromne zmęczenie materiału, podczas gdy realne zagrożenia prześlizgują się przez luki.

ISO 27001 uczy myślenia opartego na ryzyku. Zamiast pytać: *„Jak możemy zabezpieczyć wszystko?”*, pytamy: *„Co jest dla nas najważniejsze i co może nam zaszkodzić, jeśli to stracimy?”*.

Przykład z życia:

Wyobraź sobie magazyn w Twojej firmie. Masz tam dwa pomieszczenia. W jednym trzymasz zapas tonerów i papieru do drukarek. W drugim znajduje się serwerownia z bazą danych wszystkich klientów i tajnymi projektami produktów. Czy oba pomieszczenia powinny mieć identyczne zabezpieczenia?

Logiczne myślenie mówi: **Nie.** ISO 27001 pomaga organizacji uzasadnić, dlaczego na serwerownię wydajesz kupę kasy: czytniki biometryczne i monitoring, podczas gdy do magazynu tonerów wystarczą solidne drzwi i klucz.

To jest efektywność:

chronimy to, co cenne, z odpowiednią siłą.

Krótkie podsumowanie

„Manifest Architekta Bezpieczeństwa”.

„Nie jesteś już ofiarą cyberprzyszłości, jesteś jej projektantem”.

Gratulacje. Jeśli trzymasz w dłoniach ten ebook, oznacza to, że właśnie przeszedłeś najważniejszą transformację, jaką może przejść lider w cyfrowej erze.

Przestałeś postrzegać bezpieczeństwo informacyjne jako „kosztowny balast" czy „niekończące się zestawienie zakazów". Zrozumiałeś, że bezpieczeństwo to nic innego jak **architektura zaufania**.

W świecie, w którym sztuczna inteligencja potrafi podrobić głos Twojego dyrektora, a ataki hakerskie stają się tak powszechne jak deszcz, **zaufanie stało się najcenniejszą walutą**. Klienci nie kupują już tylko Twojego produktu – kupują pewność, że ich dane, ich historia i ich relacja z Twoją firmą są bezpieczne.

Jako lider, Twoim zadaniem nie jest bycie „najlepszym hakerem" w firmie. Twoim zadaniem jest bycie **Głównym Architektem Systemu Bezpieczeństwa opartego na metodologii ISO 27001**.

TO DOPIERO POCZĄTEK...

Jeżeli dotarłaś/eś do tego miejsca, oznacza to, że poznałaś/eś fundamenty bezpieczeństwa organizacji opartego na ISO 27001.

Wiesz już:

✓ dlaczego organizacje wpadają w kłopoty,

✓ czym naprawdę jest bezpieczeństwo organizacji,

✓ dlaczego informacja jest jednym z najcenniejszych aktywów,

✓ czym jest ryzyko i dlaczego nie da się go całkowicie wyeliminować,

✓ jaką rolę odgrywają ludzie, procesy i technologia,

✓ czym jest ISO 27001 i dlaczego tysiące organizacji na całym świecie wykorzystują tę normę jako fundament swojego bezpieczeństwa.

To jednak dopiero pierwszy krok.

W PEŁNEJ WERSJI PORADNIKA ZNAJDZIESZ ZNACZNIE WIĘCEJ

Pełna wersja ebooka **„Praktyczne bezpieczeństwo organizacji oparte na ISO 27001 – Część 1 Fundamenty”** zawiera:

ZNACZNIE BARDZIEJ ROZBUDOWANE TREŚCI

- szersze wyjaśnienia,
- dodatkowe przykłady,
- scenariusze z życia organizacji,
- praktyczne wskazówki dla kierownictwa,
- rozszerzone omówienie ISO 27001.

DODATKOWE ROZDZIAŁY NIEDOSTĘPNE W WERSJI BEZPŁATNEJ

Rozdział 7
Czym jest SZBI (System Zarządzania Bezpieczeństwem Informacji)

Dowiesz się, jak działa SZBI, jakie elementy powinien zawierać i dlaczego nie jest to kolejny segregator dokumentów, lecz sposób zarządzania organizacją.

Rozdział 8
Odpowiedzialność kierownictwa

Jeden z najważniejszych rozdziałów całego poradnika.

Dowiesz się:

- czego nie można delegować,
- za co odpowiada zarząd, dyrektor lub kierownik,
- dlaczego bezpieczeństwo nie jest wyłącznie zadaniem działu IT.

Rozdział 9
Pierwsze 30 dni budowy bezpieczeństwa

Gotowy plan działania krok po kroku:

- tydzień 1,
- tydzień 2,
- tydzień 3,
- tydzień 4,

oraz praktyczna checklista do wykorzystania w organizacji.

Rozdział 10
Twoja droga dalej

Dowiesz się, jak przejść od wiedzy do praktyki oraz jakie kolejne kroki warto wykonać podczas budowy bezpieczeństwa organizacji.

TO NIE JEST POJEDYNCZY EBOOK

To pierwszy tom większej serii:

PRAKTYCZNE BEZPIECZEŃSTWO ORGANIZACJI OPARTE NA ISO 27001
Seria główna (PL + EN)

📘 Część 1 – Fundamenty

📘 Część 2 – Analiza ryzyka w praktyce

📘 Część 3 – Zabezpieczenia i kontrolki

📘 Część 4 – Dokumentacja SZBI

📘 Część 5 – Audyt wewnętrzny ISO 27001

📘 Część 6 – NIS2 kontra ISO 27001

Każda kolejna część będzie rozwijała zagadnienia omawiane w tym poradniku i prowadziła czytelniczkę/czytelnika od podstaw do praktycznego wdrażania bezpieczeństwa organizacji.

Seria rozszerzona (tylko po polsku)

📗 KSC kontra ISO 27001

📗 SZBI dla szkoły publicznej (już dostępny)

📗 SZBI dla JST

📗 SZBI dla małej firmy

Dla kogo powstaje ta seria?

✓ właścicielki firm,

✓ członków zarządów,

✓ dyrektorów szkół,

✓ kierowniczek jednostek publicznych,

✓ specjalistów IT,

✓ osób odpowiedzialnych za bezpieczeństwo informacji,

✓ wszystkich, którzy chcą zrozumieć ISO 27001 bez prawniczego i normatywnego żargonu.

Chcesz otrzymać informację o kolejnych częściach?

Napisz do Wydawnictwa Cyfrowego poswojsku:

 bok@poswojsku.pl

Jeżeli szukasz konkretnego poradnika lub interesuje Ciebie wybrany temat związany z bezpieczeństwem informacji, cyberbezpieczeństwem, SZBI, NIS2, KSC lub ISO 27001 — również napisz.

Gdy tylko odpowiednia publikacja będzie dostępna, otrzymasz informację jako jedna z pierwszych osób.

Do zobaczenia w kolejnych częściach serii!

Autor: Dariusz Gołębiowski

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001

www.gddm.com.pl

Seria wydawnicza:

BEZPIECZEŃSTWO INFORMACJI CYBER AI KSC SZBI ISO 27001

Moduł 1 PODSTAWY

a już wkrótce kolejne moduły.

MODUŁ 2 Ryzyko i myślenie audytowe

MODUŁ 3 Dokumentacja, która ma sens

MODUŁ 4 Wdrożenie w praktyce

MODUŁ 5 Audyt wewnętrzny i doskonalenie

MODUŁ 6 Podsumowanie i dojrzałość

Poradniki – materiały edukacyjne dostępne będą w postaci:

A. ebooków dostępnych na poswojsku.pl

B. szkolenia elearnig zakończonego certyfikatem Audytora Wewnętrznego na portalu Akademia Bezpieczeństwa GDDM - poswojsku.com.pl

Serdecznie zapraszam do dalszego zgłębiania Twojej wiedzy i podnoszenia kompetencji w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa.

AUTOR: Dariusz Gołębiowski

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001

szkolę, doradzam, audytuję, wdrażam i porządkuję obszary: bezpieczeństwo informacji, cyberbezpieczeństwo, RODO i ryzyko informacyjne

📚 Poznaj inne książki poswojsku.pl

Jeśli spodobał się Tobie ten poradnik i chcesz dalej rozwijać swoją wiedzę o cyberbezpieczeństwie, technologii i świadomym korzystaniu z internetu, oto moje inne książki, które mogą w tym pomóc. Każda z nich powstała z myślą o osobach, które szukają praktycznych wskazówek, konkretnych przykładów i języka zrozumiałego dla każdego.

🔐 Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji – Część 1: Wprowadzenie

Kompleksowy wstęp do tematyki ochrony danych, prywatności i bezpiecznego korzystania z sieci. To książka dla tych, którzy chcą szybko zrozumieć, na czym polegają najważniejsze zagrożenia i jak zacząć się przed nimi skutecznie bronić – bez skomplikowanego żargonu. Znajdziesz tu przykłady z życia i proste instrukcje krok po kroku.

🛡️ Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji – Część 2: Cyberhigiena

Praktyczny przewodnik po codziennych nawykach, które realnie zwiększają Twoje bezpieczeństwo. Dowiesz się, jak tworzyć silne hasła, chronić urządzenia, wykrywać próby oszustw i przygotować swoją rodzinę na zagrożenia cyfrowe. To pozycja obowiązkowa, jeśli chcesz, żeby cyberhigiena była naturalną częścią Twojego życia.

👨‍👧‍👦 Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji – Część 3: Dziecko i Ty

Poradnik stworzony specjalnie dla rodziców i opiekunów, którzy chcą wprowadzać dzieci w cyfrowy świat z rozsądkiem i spokojem. Znajdziesz tu nie tylko zasady i rekomendacje, ale też gotowe sposoby rozmowy o bezpieczeństwie i budowania zaufania. Ta książka pomoże Ci chronić najmłodszych bez straszenia i nadmiernej kontroli.

🤖 AI w edukacji – Część 1: Praktyczny poradnik nie tylko dla nauczycieli

Sztuczna inteligencja to nie tylko moda, ale i realne narzędzie, które może usprawnić naukę i pracę. W tej książce pokazuję, jak korzystać z AI w prosty sposób – od generowania treści, przez wspieranie kreatywności, po automatyzację codziennych zadań. Idealna dla edukatorek/edukatorów i osób, które chcą poznać podstawy nowoczesnych technologii.

✨ AI w edukacji – Część 2: Praktyczne pomysły na kreatywną edukację

Kontynuacja pierwszej części – pełna inspiracji, scenariuszy zajęć i ćwiczeń. Dowiesz się, jak prowadzić warsztaty i lekcje, które łączą AI z rozwojem kompetencji cyfrowych, logicznego myślenia i twórczego podejścia do nauki. Świetna pozycja dla wszystkich, którzy szukają konkretnych narzędzi i gotowych rozwiązań.

🕹️ Stwórz Grę Mobilną

Praktyczny przewodnik dla osób, które marzą o stworzeniu własnej gry na smartfon. Od absolutnych podstaw programowania w JavaScript i React Native, przez projektowanie rozgrywki, aż po publikację gry. Jeśli chcesz uczyć się kodowania w sposób ciekawy i namacalny, to ta książka będzie Twoim drogowskazem.

🌿 Saga CyberJestestwa

Powieść science fiction dla tych, którzy chcą oderwać się od codzienności i zanurzyć w refleksyjnej historii o sensie istnienia, wolności i relacjach w obliczu zmian. To opowieść o ludziach i technologii, o wyborach i konsekwencjach – dla miłośniczek/miłośników literatury, którzy cenią głębsze przesłanie i oryginalny klimat.

Wszystkie moje ebooki możesz nabyć na:

📍 stronie wydawnictwa cyfrowego **poswojsku.pl**

🎓 Szkolenia i Webinary

Jeśli chcesz pogłębić wiedzę, zdobyć praktyczne umiejętności i od razu wprowadzić je w życie – zapraszam Cię na moje szkolenia i webinary. Każde z nich zostało przygotowane tak, aby w przystępny sposób przekazać konkretne rozwiązania i pomóc Ci działać od zaraz.

🔒 Bezpieczni w sieci – Jak chronić siebie i rodzinę przed cyberzagrożeniami

Szkolenie, w którym krok po kroku omawiam zagrożenia najczęściej dotykające rodziny – od fałszywych wiadomości i wyłudzeń danych, po ochronę urządzeń domowych i zabezpieczanie dzieci w internecie. Idealne dla rodziców, opiekunów i osób, które chcą działać świadomie.

💼 Cyberbezpieczeństwo dla małych organizacji i firm

Praktyczny warsztat dla właścicieli firm, fundacji i urzędów, którzy chcą nauczyć się chronić dane pracowników i klientów bez kosztownych wdrożeń. Omawiam darmowe narzędzia, procedury bezpieczeństwa i sposoby budowania kultury cyberhigieny w zespole.

🧠 AI w życiu codziennym – od podstaw

Webinar pokazujący, jak sztuczna inteligencja może ułatwić pracę, naukę i organizację codziennych spraw. Dowiesz się, jak korzystać z AI do tworzenia treści, automatyzacji zadań i rozwijania nowych umiejętności – nawet jeśli nie masz doświadczenia technicznego.

🔑 Szyfrowanie danych – dyski, pliki, poczta

Szkolenie wprowadzające w świat szyfrowania, pokazujące krok po kroku, jak zabezpieczyć swoje dane prywatne i firmowe za pomocą bezpłatnych narzędzi. Idealne dla każdego, kto chce uniknąć utraty poufnych informacji.

👧 **Cyfrowe bezpieczeństwo dziecka – jak mądrze wspierać młodych użytkowników internetu**

Spotkanie dla rodziców i nauczycieli, którzy chcą dowiedzieć się, jak rozmawiać z dziećmi o zagrożeniach online, jak ustawiać kontrolę rodzicielską i jak budować zaufanie w cyfrowym świecie.

Aktualne terminy szkoleń i webinarów znajdziesz na stronie: 🌐 poswojsku.pl

a webinarów: www.poswojsku.com.pl

Zapraszam również do kontaktu – chętnie pomogę dobrać szkolenie odpowiednie dla Twoich potrzeb.

🌟 ***Zostańmy w kontakcie!***

Jeśli chcesz być na bieżąco z nowymi książkami, szkoleniami i inspiracjami o cyberbezpieczeństwie, technologii i AI – zapraszam Cię do obserwowania moich profili. Dzięki temu nie przegapisz premier, promocji i wartościowych materiałów które tworzę: często, prosto, przystępnie i z humorem.

- ***Strona internetowa*** 📍 ***poswojsku.pl***
- ***Facebook*** 📍 ***facebook.com/poswojsku***
- ***YouTube*** 📍 ***youtube.com/@poswojsku***
- ***LinkedIn*** 📍 ***linkedin.com/in/golebiowski-dariusz***
- ***Instagram*** 📍 ***instagram.com/poswojsku***
- ***Threads*** 📍 ***threads.com/@poswojsku***
- ***TikTok*** 📍 ***tiktok.com/@astilus***
- ***Amazon Author Page*** 📍 ***amazon.com/author/dariuszgolebiowski***
- ***Goodreads*** 📍 ***goodreads.com/dariuszgolebiowski***

Proszę, dołącz do mnie – razem budujmy bezpieczniejszy i bardziej świadomy świat cyfrowy!