



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



SYSTEM ZARZĄDZANIA BEZPIECZETWEM INFORMACJI według PN-EN ISO/IEC 27001:2007

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



DLACZEGO CHRONIMY INFORMACJE?

- ❖ informacja należy do aktywów organizacji
- ❖ strategiczne znaczenie informacji dla organizacji
- ❖ informacja – element procesów biznesowych
- ❖ przepisy prawne nakazujące ochronę informacji
- ❖ umowy wymagające ochrony informacji



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



PRZYKŁADOWE KATEGORIE INFORMACJI:

- ❖ informacje jawne
- ❖ informacje chronione (zastrzeżone)
- ❖ informacje poufne
- ❖ informacje tajne



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



ZASOBY ORGANIZACJI:

- ❖ zasoby informacyjne (bazy danych, dokumenty)
- ❖ zasoby fizyczne (budynki, urządzenia informatyczne, urządzenia komunikacyjne)
- ❖ oprogramowanie
- ❖ pracownicy
- ❖ zdolność wytwarzania lub świadczenia usług
- ❖ dobra niematerialne (wizerunek, reputacja)

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



PRZYKŁADY INFORMACJI WRAŻLIWEJ:

- ❖ informacje chronione w związku z obowiązującym przepisami prawnymi
- ❖ informacje chronione w związku z nakazem organów kompetentnych (np. ABW)
- ❖ informacje, które stają się wrażliwe w zestawieniu z innymi informacjami (np. informacje dotyczące spotkań kierownictwa, planów wyjazdów służbowych zamówionych analiz innych firm)
- ❖ informacje dotyczące życia osobistego najwyższego kierownictwa firmy (wywołanie skandalu, szantaż itp.)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

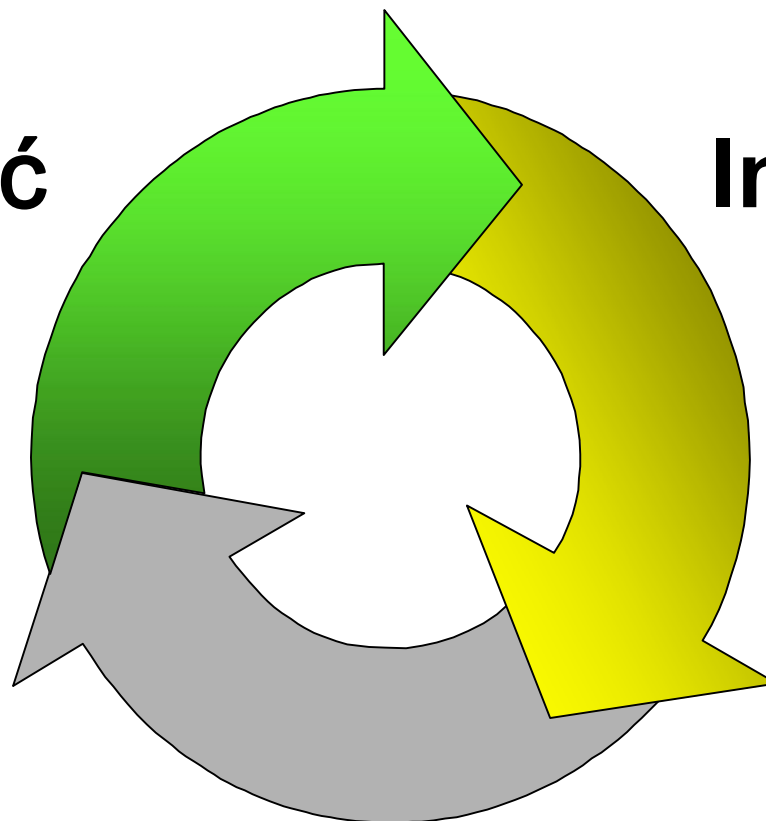
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



PODSTAWOWE ATRYBUTY INFORMACJI

Poufność

Integralność



Dostępność

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



CO TO SĄ ZAGROŻENIA?

Zagrożenie:

potencjalna przyczyna niepożądanego incydentu,
którego skutkiem może być szkoda dla systemu lub
instytucji

(ISO/IEC 13335-1:2004)

Zagrożenie:

potencjalna możliwość naruszenia bezpieczeństwa
systemu informatycznego

(PN-I-02000: 2002)

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



GŁÓWNE ATRYBUTY ZAGROŻEŃ TO:

- ❖ źródło pochodzenia (wewnętrzne, zewnętrzne)
- ❖ motywacja (np. korzyści finansowe)
- ❖ dotkliwość
- ❖ częstotliwość pojawiania się
- ❖ szkodliwość



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



PODSTAWOWE KLASY ZAGROŻEŃ BEZPIECZEŃSTWA INFORMACJI

- ❖ działania przestępcze
- ❖ skutki złej organizacji pracy
- ❖ błędy personelu obsługującego system komputerowy
- ❖ awarie sprzętu i wady oprogramowania
- ❖ siły wyższe

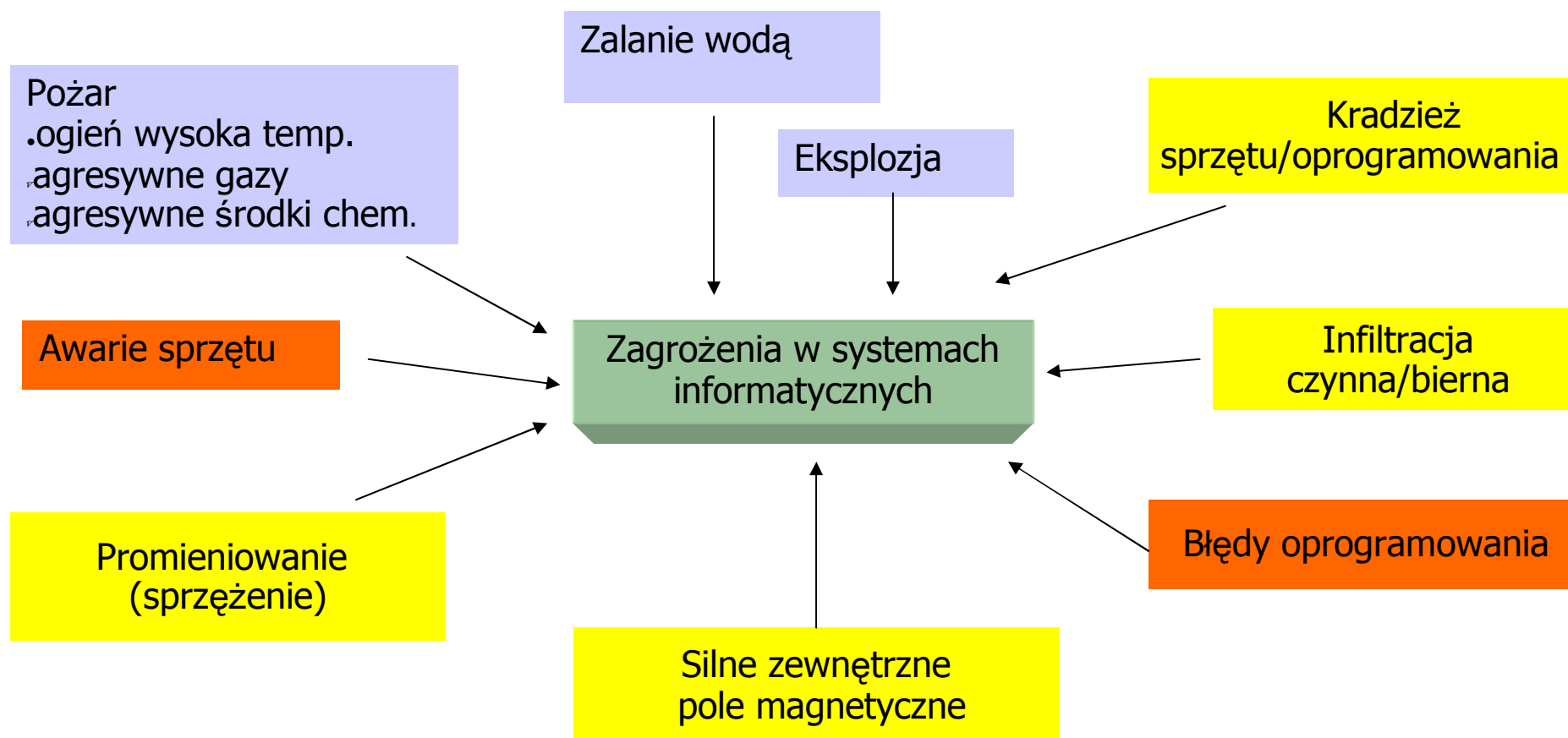


KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



ZAGROŻENIA INFORMACJI PRZETWARZANYCH W SYSTEMACH KOMPUTEROWYCH



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

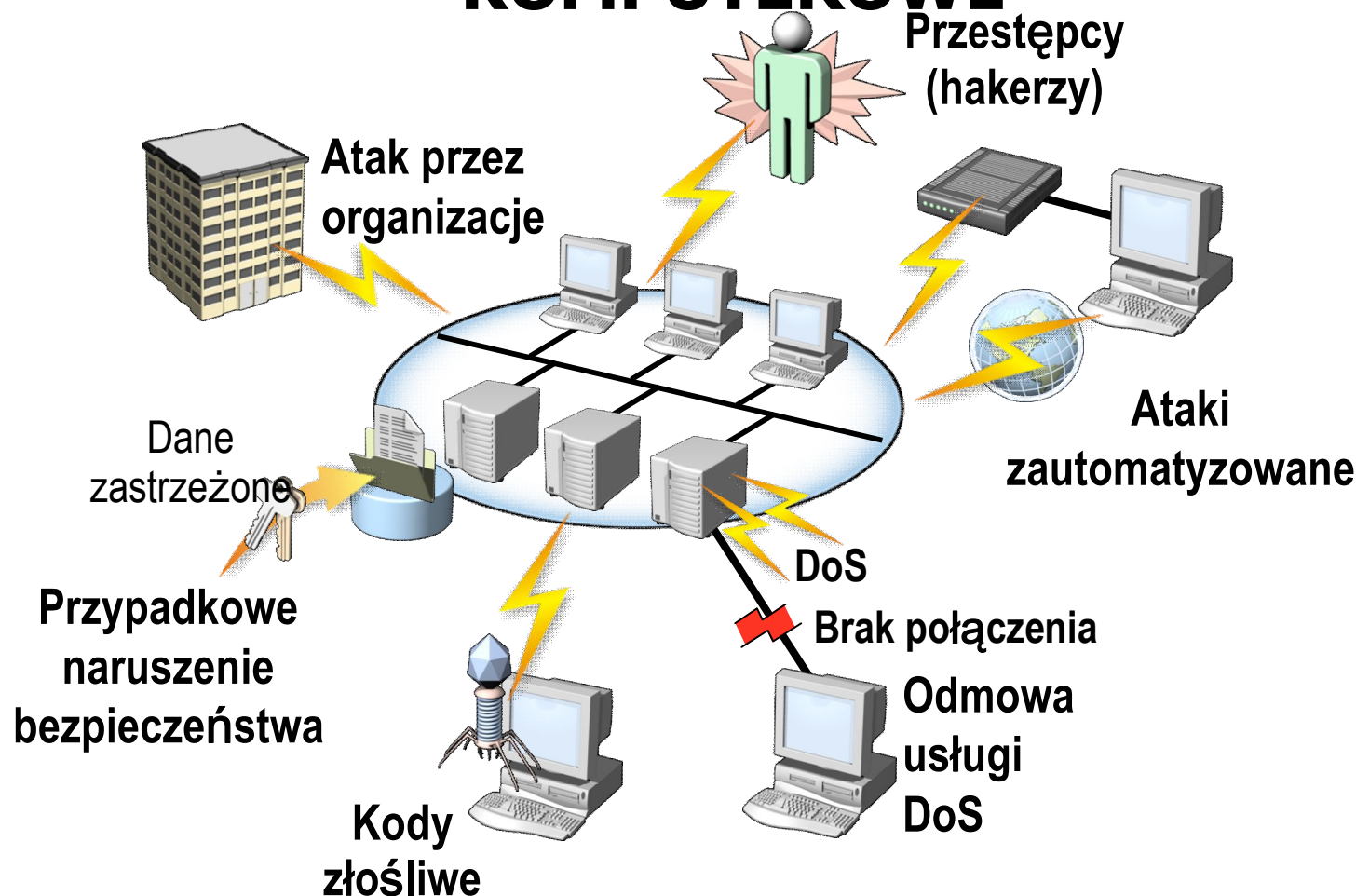


KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



PODSTAWOWE TYPY ATAKÓW NA SIECI KOMPUTEROWE



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



PODATNOŚĆ:

wady lub luki w strukturze fizycznej organizacji, procedurach, zarządzaniu, administrowaniu, sprzęcie, oprogramowaniu, a także zamierzone lub niezamierzone działania personelu, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika

Uwagi:

- ❖ istnienie podatności nie powoduje szkód samo z siebie. Podatność jest jedynie warunkiem lub zestawem warunków, które umożliwiają uszkodzenie systemu lub zakłócenie działalności użytkownika przez atak
- ❖ jeżeli podatność odpowiada zagrożeniu, to istnieje ryzyko



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



CO TO JEST RYZYKO?

Ryzyko

możliwość, że konkretne zagrożenie wykorzysta konkretną podatność systemu przetwarzania danych
(PN-I 02000:2002)

Ryzyko

prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów
(ISO/IEC 13335-1:2004)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



CO TO JEST RYZYKO?

Ryzyko

można zdefiniować jako iloczyn prawdopodobieństwa zdarzenia i miary strat spowodowanych tym zdarzeniem (albo wartości aktywu)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



CO TO JEST ZABEZPIECZENIE?

Zabezpieczenie

praktyka, procedura lub mechanizm redukujący ryzyko

Cel zabezpieczeń: ochrona przed zagrożeniami,
ograniczenie podatności, minimalizowanie następstw,
wykrywanie błędów i nieprawidłowości, wsparcie w
trakcie ewentualnego odtwarzania systemu



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Niektóre funkcje zabezpieczeń:

- ❖ zapobieganie
- ❖ ograniczanie
- ❖ wykrywanie
- ❖ monitorowanie
- ❖ odtwarzanie
- ❖ poprawianie
- ❖ uświadamianie



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Przykładowe zabezpieczenia systemów informatycznych:

- ❖ mechanizmy kontroli dostępu
- ❖ szyfrowanie
- ❖ podpisy cyfrowe
- ❖ oprogramowanie antywirusowe
- ❖ sieciowe zapory ogniowe
- ❖ kopie zapasowe
- ❖ zasilanie rezerwowe

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



System zarządzania bezpieczeństwem informacji (SZBI)

(Information Security Management System – ISMS)

Jest to ta część systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji

UWAGA: System zarządzania zawiera strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i zasoby
(PN-ISO/IEC 27001:2007)

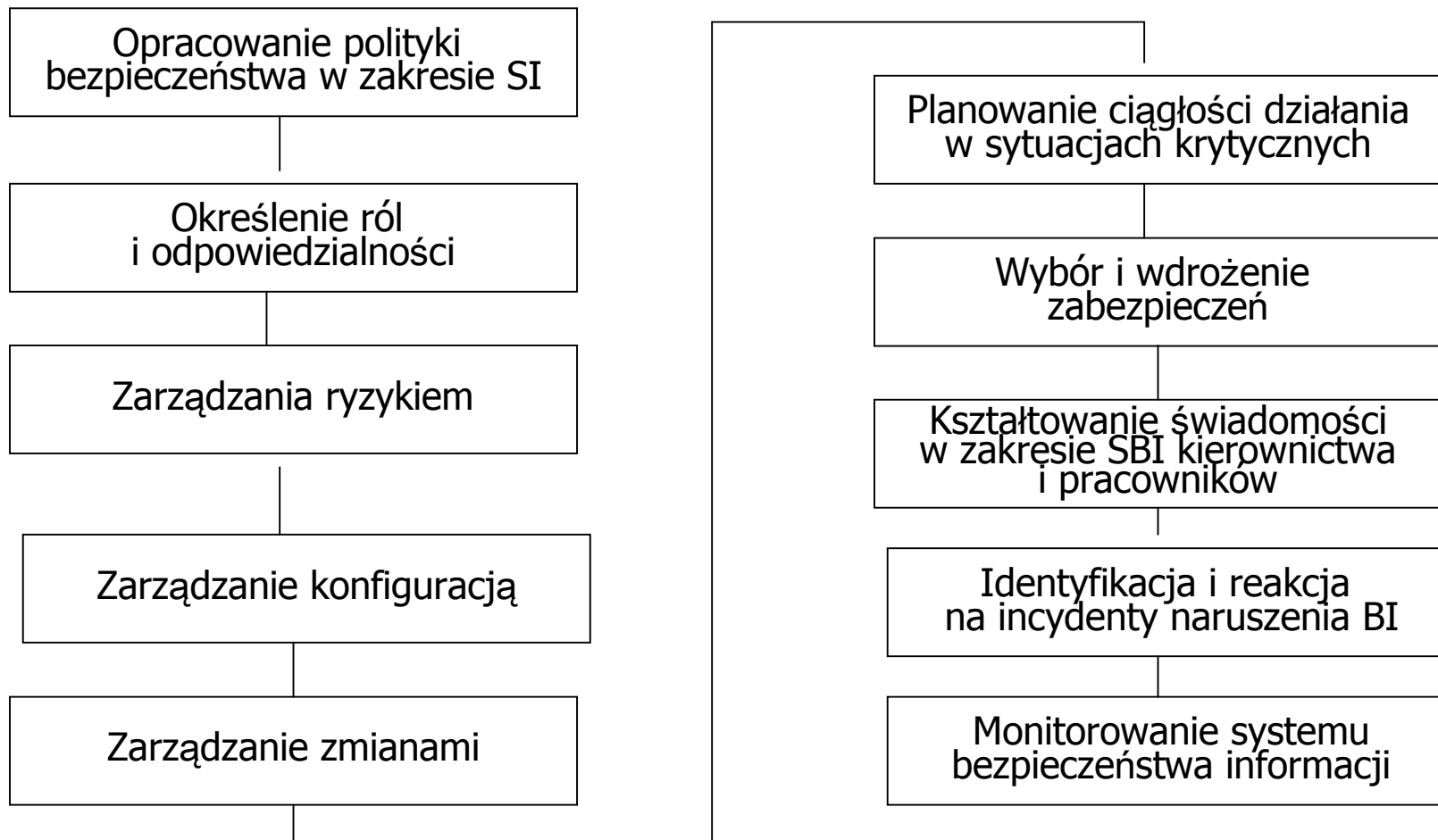


KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Proces zarządzania bezpieczeństwem systemów informatycznych



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Polityka bezpieczeństwa w zakresie systemów informatycznych:

Zasady, zarządzenia i procedury, które określają, jak zasoby – włącznie z informacjami wrażliwymi – są zarządzane, chronione i dystrybuowane w instytucji i jej systemami informatycznymi (*ISO/IEC 13335-1:2004*)

Określone działania, mające doprowadzić do osiągnięcia założonych celów.

W organizacji określane i realizowane są różnorodne polityki, np.:

- ❖ polityka kadrowa
- ❖ polityka bezpieczeństwa osobowego
- ❖ polityka w zakresie bezpieczeństwa fizycznego
- ❖ polityka bezpieczeństwa energetycznego
- ❖ polityka zabezpieczenia ciągłości działania w organizacji



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



DOKUMENT POLITYKI BEZPIECZEŃSTWA INFORMACJI ORGANIZACJI:

zbiór dokumentów, na podstawie których można, np.:

- ❖ oceniać zidentyfikowane zagrożenia
- ❖ podejmować odpowiednie działania
- ❖ klasyfikować poziom dostępu do informacji
- ❖ określać zasady uzyskiwania fizycznego dostępu do pomieszczeń, w których są przetwarzane informacje



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Forum Bezpieczeństwa Informacji – podstawowe zadania:

- ❖ współudział w formułowaniu polityki BI
- ❖ współudział w formułowaniu planu BI
- ❖ określenie zasobów niezbędnych do wdrożenia procesów BI
- ❖ opracowanie planu wdrażania przedsięwzięć BI
- ❖ nadzór nad wdrażaniem planu BI
- ❖ ustalenie zakresów obowiązków pracowników odpowiedzialnych za BI
- ❖ nadzór nad informowaniem pracowników o działaniach w zakresie BI
- ❖ kontrola efektywności przedsięwzięć BI w toku pracy organizacji

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Pełnomocnik ds. bezpieczeństwa informacji – podstawowe obowiązki:

- ❖ opracowanie koncepcji bezpieczeństwa organizacji
- ❖ współudział w opracowaniu koncepcji bezpieczeństwa informatycznego organizacji w zgodności z koncepcją kompleksowego bezpieczeństwa organizacji
- ❖ kierowanie zespołem ochrony
- ❖ informowanie kierownictwa organizacji i FBI o przebiegu procesów wdrażania i utrzymania SZBI
- ❖ określenie dróg przepływu informacji do lokalnych pełnomocników oraz analiza tych informacji
- ❖ nadzór nad wykonywaniem zadań przez administratorów BI
- ❖ planowanie i nadzorowanie szkoleń w zakresie BI
- ❖ analiza i reakcja na incydenty naruszające BI



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



ZARZĄDZANIE RYZYKIEM

Identyfikacja:

- ❖ zasobów podlegających ochronie i ich klasyfikacja
- ❖ zagrożeń

Określenie:

- ❖ podatności
- ❖ następstw,
- ❖ zabezpieczeń
- ❖ ryzyka
- ❖ ryzyka szczątkowego



Proces zarządzania ryzykiem





KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



USTALENIE WARUNKÓW POCZĄTKOWYCH:

- ❖ identyfikacja aktywów informacji
- ❖ określenie wartości aktywów informacji
- ❖ podział aktywów na klasy (w zależności od wagi dla organizacji)
- ❖ określenie zasad szacowania ryzyka
- ❖ powołanie zespołu do przeprowadzenia szacowania ryzyka.



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



ANALIZA RYZYKA

Identyfikacja ryzyka

- ❖ Najczęściej stosowane techniki:
- ❖ analiza środowiskowa (ocena wpływu zmian środowiska zewnętrznego na procesy zarządzania i kontroli w organizacji)
- ❖ scenariusze zagrożeń (symulowanie zagrożeń i słabości systemu kontroli wewnętrznej organizacji)
- ❖ analiza potencjalnych strat (ocena z punktu widzenia organizacji)
- ❖ identyfikacja systemowa (ocena wpływu wszystkich potencjalnych czynników ryzyka)

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



PRZYDZIELENIE WAG – WAGA KONSEKWENCJI

Przy ocenie wartości zasobów informacyjnych bierze się pod uwagę czynniki, takie jak:

- ❖ zobowiązania prawne i regulaminowe organizacji
- ❖ wymagania obowiązujących przepisów prawa
- ❖ interesy handlowe i ekonomiczne organizacji
- ❖ konsekwencje finansowe w przypadku utraty ciągłości działania
- ❖ bezpieczeństwo osobiste i poufne informacje osobiste
- ❖ polityka działania organizacji
- ❖ utrata reputacji
- ❖ porządek publiczny



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



OCENA RYZYKA

Ocena ryzyka wieńczy proces szacowania ryzyka

- ❖ przyjęcie metody oceny ryzyka
- ❖ przeprowadzanie obliczeń
- ❖ określenie prawdopodobieństwa ryzyka w liczbach
- ❖ podział na kategorie (zwykle stosuje się 5 kategorii w zależności od wielkości wyliczonego prawdopodobieństwa: bardzo wysokie, wysokie, średnie, niskie, pomijalne)

Konfrontacja wyliczonego ryzyka ze skutkami pozwala na określenie wag ryzyka



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



PLAN POSTĘPOWANIA Z RYZYKIEM

Postępowanie z ryzykiem:

- ❖ akceptowanie ryzyka
- ❖ kontrolowanie ryzyka
- ❖ ograniczenie ryzyka (np. zastosowanie zabezpieczeń)
- ❖ przeniesienie ryzyka (np. ubezpieczenie)
- ❖ unikanie ryzyka

W załączniku A do normy PN-ISO/IEC 27001:2007 podano przykładowe cele stosowania zabezpieczeń i zabezpieczenia



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



AKCEPTOWANIE RYZYKA SZCZĄTKOWEGO

Decyzję o akceptowaniu ryzyka szczątkowe podejmuje kierownictwo organizacji

Decyzja jest arbitralna i podejmowana w oparciu o wyniki procesu szacowania ryzyka

Przy podejmowaniu decyzji należy mieć świadomość, że ocena ryzyka oparta jest w dużym stopniu na subiektywnych miarach i ocenach. Dlatego też bardzo ważnym jest staranne dobranie analityków do zespołu wykonującego szacowanie ryzyka



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



ZARZĄDZANIE KONFIGURACJĄ

Proces weryfikacji zmian w SZBI

- ❖ wprowadzenie zmian, które nie powinny obniżać efektywności funkcjonowania systemu, skuteczności zastosowanych mechanizmów zabezpieczających oraz ogólnego bezpieczeństwa organizacji
- ❖ wprowadzenie stosownych zmian dotyczących planowania ciągłości działania i odtwarzania po katastrofie



Proces zarządzania konfiguracją obejmuje:

- ❖ procedury gwarantujące, że rejestr zasobów zawiera wyłącznie istniejące i autoryzowane składniki konfiguracji
- ❖ procedury zapewniające rejestrację wszelkich zmian konfiguracji
- ❖ określenie konfiguracji wzorcowej – punktu kontrolnego używanego do ewentualnego powrotu po zmianach
- ❖ politykę zarządzania wersjami
- ❖ procedury sprawdzania legalności oprogramowania
- ❖ procedury stosowania oprogramowania antywirusowego
- ❖ procedury przechowywania oprogramowania
- ❖ procedury inwentaryzacji zasobów organizacji



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



ZARZĄDZANIE ZMIANAMI

Identyfikowanie nowych wymagań w zakresie bezpieczeństwa związanych z wprowadzanymi zmianami w systemie informatycznym

Systemy informatyczne podlegają ciągłym zmianom w wyniku pojawiania się nowych zagrożeń i podatności w związku z rozwojem usług i technologii



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



ZARZĄDZANIE ZMIANAMI

Każda planowana zmiana w systemie informatycznym powinna być poddana analizie pod kątem jej wpływu na bezpieczeństwo, z uwzględnieniem związanych z nią rodzajów ryzyka oraz potencjalnych zysków i strat

Ustalenia powinny być udokumentowane

Skuteczny proces zarządzania zmianami zapewnia spójność infrastruktury informatycznej, odpowiedni poziom bezpieczeństwa informacji przy projektowaniu nowych rozwiązań oraz wdrożenie komponentów o wysokiej jakości



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Procedury wprowadzania zmian w infrastrukturze powinny obejmować:

- ❖ zasady planowania infrastruktury informatycznej w organizacji
- ❖ zasady planowania wprowadzanych zmian
- ❖ zasady definiowania wymagań funkcjonalnych dla nowych lub modyfikowanych komponentów
- ❖ wymagania w zakresie mechanizmów bezpieczeństwa, które powinny posiadać nowe lub modyfikowane komponenty oraz metody ich sprawdzania
- ❖ zasady analizowania zgodności nowych komponentów z pozostałymi elementami systemu informatycznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



PLANOWANIE CIĄGŁOŚCI DZIAŁANIA W SYTUACJACH KRYTYCZNYCH

Ciągłość działania:

utrzymanie niezbędnych usług systemu informatycznego po poważnej awarii w centrum informatycznym, która może być spowodowana przyczynami naturalnymi, takimi jak pożar lub trzęsienie ziemi, lub zdarzeniem wywołanym rozmyślnie, np. sabotaż

(PN-I-02000:2002)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Zagrożenia ciągłości działania to między innymi:

- ❖ awaria sprzętu komputerowego
- ❖ awaria serwerów
- ❖ awaria sieci komputerowej
- ❖ awaria zasilania
- ❖ klęski żywiołowe
- ❖ włamanie do firmy z zewnątrz; włamanie fizyczne (złodzieje),
włamanie poprzez sieć informatyczną (hakerzy)
- ❖ pożar
- ❖ powódź
- ❖ katastrofa budowlana



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



WYBÓR I WDROŻENIE ZABEZPIECZEŃ

Zabezpieczenia to praktyki, procedury lub mechanizmy, które mogą chronić przed zagrożeniem, redukować podatność, ograniczać następstwa, wykrywać niepożądane incydenty i ułatwiać odtwarzanie

Odpowiedni dobór zabezpieczeń jest kluczowy dla prawidłowego wdrożenia polityki bezpieczeństwa

Efektywna ochrona wymaga zwykle kombinacji różnych zabezpieczeń w celu utworzenia warstw ochronnych dla zasobów



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



PRZYKŁADOWE OBSZARY UŻYCIA ZABEZPIECZEŃ:

- ❖ środowisko fizyczne
- ❖ środowisko techniczne (sprzęt komputerowy, oprogramowanie, urządzenia komunikacyjne),
- ❖ personel
- ❖ administracja



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



PRZYKŁADOWE ZABEZPIECZENIA:

- ❖ mechanizmy kontroli dostępu
- ❖ oprogramowanie antywirusowe
- ❖ szyfrowanie w celu uzyskania poufności
- ❖ podpisy cyfrowe
- ❖ sieciowe zapory ogniowe
- ❖ narzędzia monitoringu i analizy sieci
- ❖ zasilanie rezerwowe
- ❖ kopie zapasowe



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Identyfikacja i reakcja na incydenty naruszenia bezpieczeństwa informacji

Każde zdarzenie związane bezpośrednio z systemem z systemem informatycznym, które umożliwia nieuprawniony dostęp do informacji przetwarzanej, przesyłanej i przechowywanej w systemie, umożliwia lub powoduje utratę jej integralności i/lub dostępności uważane jest za **incydent naruszenia bezpieczeństwa informacji**

Incydent - zrealizowane zagrożenie



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Identyfikacja i reakcja na incydenty naruszenia bezpieczeństwa informacji

Reagowanie na naruszenie bezpieczeństwa i niewłaściwego funkcjonowania systemu ma na celu minimalizowanie uszkodzeń będących skutkiem tego naruszenia i niewłaściwego działania oraz monitorowanie i wyciąganie wniosków z takich przypadków

Przypadki naruszenia bezpieczeństwa powinny być zgłaszane poprzez właściwe kanały tak szybko jak to możliwe.

Powinny być opracowane i wdrożone procedury zgłaszania i reagowania na wystąpienie danego naruszenia (incydentu), w których określono działania podejmowane po otrzymaniu zgłoszenia o naruszeniu.



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Reagowanie na incydenty naruszenia bezpieczeństwa na poziomie strategicznym – działania powinny być zrealizowane przed wystąpieniem incydentu

W organizacji powinny być określone osoby odpowiedzialne za podejmowanie bieżących decyzji strategicznych

Należy rozstrzygnąć, czy będą przekazywane poza organizację informacje o zaistniałym incydencie wraz z wytycznymi dla wyznaczonych pracowników

Należy rozstrzygnąć, czy i w jakich przypadkach będą powiadamiane organy państwowe (policja, prokuratura, ABW)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Należy rozstrzygnąć, czy firma będzie korzystać z pomocy zewnętrznych specjalistów

Określenie działań w przypadku zidentyfikowania intruza

Wytyczne dla obsługi technicznej odnośnie taktyki reakcji na włamanie do systemu (uniemożliwienie działań intruza, zebranie dowodów przeciwko intruzowi, nawet kosztem pewnych strat w systemie)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



REAGOWANIE NA INCYDENTY NARUSZENIA BEZPIECZEŃSTWA NA POZIOMIE TECHNICZNYM

W organizacji powinien być powołany zespół odpowiedzialny za reakcję na incydenty, składających się z kompetentnych specjalistów posiadających wiedzę w zakresie odpowiednich technologii adekwatnych do analizowanego systemu oraz procesu dochodzenia i metod zbierania śladów nieuprawnionej działalności



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



DZIAŁANIA PRZED WYSTĄPIENIEM INCYDENTU:

- ❖ przygotowanie i przeszkolenie zespołu obsługującego incydenty (zabezpieczenie śladów działania intruza usuwanie powstałych w systemie szkód)
- ❖ przygotowanie zestawu narzędzi (programowych i sprzętowych) wykorzystywanych przy obsłudze incydentu
- ❖ przygotowanie metodyki obsługi incydentu
- ❖ przygotowanie komputerów w chronionym systemie
- ❖ przygotowanie sieci komputerowej



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



DZIAŁANIA PO WYSTĄPIENIU INCYDENTU:

- ❖ zebranie ulotnych danych
- ❖ wykonanie duplikatu systemu
- ❖ przeprowadzenie dochodzenia (najlepiej na duplikacie systemu), zebranie i udokumentowanie śladów działań intruza
- ❖ wyizolowanie i opanowanie incydentu
- ❖ wprowadzenie dodatkowych zabezpieczeń – usunięcie podatności wykorzystanych podczas incydentu
- ❖ odtworzenie systemu (kopia bezpieczeństwa może zawierać nazwy użytkowników i hasła wykorzystane podczas ataku)
- ❖ dokumentowanie wszystkich przeprowadzonych działań
- ❖ sporządzenie raportów końcowych



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



DZIAŁANIA PO WYSTĄPIENIU INCYDENTU:

Zgłaszanie słabości systemu bezpieczeństwa (zgłaszanie przez użytkowników wszelkich zauważonych lub podejrzewanych słabości systemów i usług lub zagrożeń z nimi związanych

Zgłaszanie niewłaściwego funkcjonowania oprogramowania:

- ❖ odnotowanie objawów i wszelkich komunikatów pojawiających się na ekranie
- ❖ odizolowanie komputera
- ❖ natychmiastowe zgłoszenie problemu kierownikowi odpowiedzialnemu za bezpieczeństwo informacji



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



DZIAŁANIA PO WYSTĄPIENIU INCYDENTU:

Analizowanie zapisów z incydentów naruszenia bezpieczeństwa informacji i podjętych działań w celu podjęcia działań, mających na celu uniknięcie w przyszłości podobnych problemów

Organizacja powinna opracować procedurę postępowania dyscyplinarnego wobec osób, które przyczyniły się do naruszenia bezpieczeństwa chronionej informacji

Wykorzystanie przeprowadzonych analiz w celach edukacyjnych i do podnoszenia poziomu bezpieczeństwa informacji



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



MONITOROWANIE SYSTEMU BEZPIECZEŃSTWA INFORMACJI

Pomiar lub szacowanie wykonania procedur i wymogów polityki bezpieczeństwa

Działania mają na celu potwierdzenie, że wdrożone zabezpieczenia funkcjonują efektywnie i zgodnie z zamierzeniami a ISMS pozostaje skuteczny

Podejmowanie działań korygujących, mających na celu utrzymanie spójności dokumentacji ISMS z realizowanymi działaniami oraz niedopuszczenie do narażenia organizacji na nieakceptowalne ryzyko



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



TECHNIKI STOSOWANE W MONITOROWANIU:

- ❖ rutynowe sprawdzani
- ❖ samokontrolujące procedury
- ❖ audyty wewnętrzne ISMS
- ❖ uczenie się od innych
- ❖ przeglądy wykonywane przez kierownictwo
- ❖ analizy trendów



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



STRUKTURA NORMY PN-ISO/IEC 27001

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

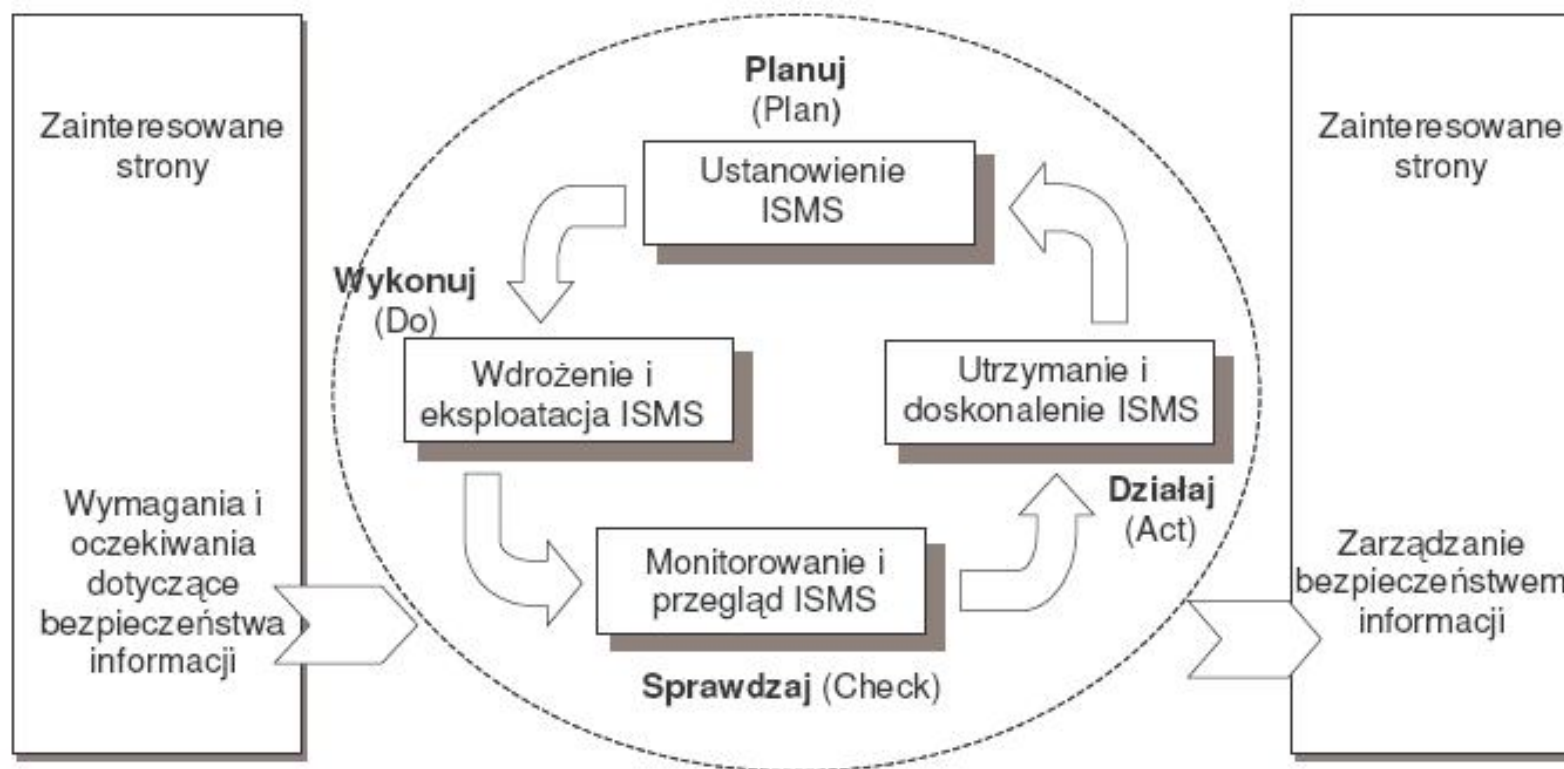


0. Wprowadzenie
1. Zakres normy
2. Powołania normatywne
3. Terminy i definicje
4. System zarządzania bezpieczeństwem informacji (SZBI)
5. Odpowiedzialność kierownictwa
6. Wewnętrzne audyty ISMS
7. Przeglądy SZBI realizowane przez kierownictwo
8. Doskonalenie SZBI

Załącznik A Cele stosowania zabezpieczeń i zabezpieczenia



MODEL PDCA STOSOWANY W PROCESACH SZBI





KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



3. TERMINY I DEFINICJE

Informacja:

obiekt abstrakcyjny, który w postaci zakodowanej (dane) może być przechowywany (na nośniku danych), przesyłany, przetwarzany, użyty do sterowania

(Encyklopedia Powszechna PWN)

Informacja:

znaczące dane

(PN-EN ISO 9000:2005)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



3. TERMINY I DEFINICJE

Dane:

reprezentacja (kod) informacji

(Encyklopedia Powszechna PWN)

Dokument:

informacja i jej nośnik

(PN-EN ISO 9000:2005)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



3. TERMINY I DEFINICJE

Aktywa:

wszystko co ma wartość dla organizacji

(ISO/IEC 13335-1:2004)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



3. TERMINY I DEFINICJE

Bezpieczeństwo informacji:

zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność
(ISO/IEC 17799:2005)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



3. TERMINY I DEFINICJE

Poufność:

właściwość, że informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom lub procesom

(ISO/IEC 13335-1:2004)

Integralność:

właściwość zapewnienia dokładności i kompletności aktywów

(ISO/IEC 13335-1:2004)



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



3. TERMINY I DEFINICJE

Dostępność:
właściwość bycia dostępnym
i użytecznym na żądanie upoważnionego podmiotu

(ISO/IEC 13335-1:2004)



3. TERMINY I DEFINICJE

Informacja wrażliwa:

informacja, która zgodnie z ustaleniem organu kompetentnego ma być chroniona, ponieważ jej nieuprawnione ujawnienie, zmiana, zniszczenie lub utrata spowoduje zauważalne szkody dla kogoś lub czegoś

(PN-I-02000: 2002)

Informacje wrażliwe dla organizacji są to informacje, które mogą zostać wykorzystane przeciwko interesom tej organizacji przez ujawnienie, nieudostępnienie, zmianę lub zniszczenie w sposób nieautoryzowany



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



4. SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI)

4.2 Ustanowienie i zarządzanie SZBI

4.2.1 Ustanowienie SZBI



4.2.1 USTANOWIENIE SZBI

- ❖ zdefiniowanie zakresu i granic SZBI
- ❖ zdefiniowanie polityki SZBI
- ❖ zdefiniowanie podejścia do szacowania ryzyka w organizacji
- ❖ określenie ryzyka
- ❖ analiza i ocena ryzyka



4.2.1 USTANOWIENIE SZBI

- ❖ zdefiniowanie wariantów postępowania z ryzykiem
- ❖ wybór celów stosowania zabezpieczeń
- ❖ akceptacja kierownictwa dla ryzyk szczytkowych
- ❖ uzyskanie autoryzacji kierownictwa do wdrażania SZBI
- ❖ przygotowanie deklaracji stosowania



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



4.2.2 WDROŻENIE I EKSPLOATACJA SZBI

- ❖ sformułowanie planów postępowania z ryzykiem
- ❖ wdrożenie planu postępowania z ryzykiem
- ❖ wdrożenie zabezpieczeń



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



4.2.2 WDROŻENIE I EKSPLOATACJA SZBI

- ❖ zdefiniowanie pomiarów wybranych zabezpieczeń
- ❖ wdrożenie programów szkoleń
- ❖ zarządzanie eksploatacją SZBI
- ❖ natychmiastowa reakcja na incydenty związane z naruszeniem bezpieczeństwa



4.2.3 MONITOROWANIE I PRZEGLĄD SZBI

- ❖ procedury monitorowania, przeglądu i innych zabezpieczeń
- ❖ regularne przeglądy skuteczności SZBI
- ❖ pomiary skuteczności zabezpieczeń
- ❖ przeglądy szacowania ryzyka



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



4.2.3 MONITOROWANIE I PRZEGLĄD SZBI

- ❖ audyty wewnętrzne SZBI w zaplanowanych odstępach czasu
- ❖ przeglądy SZBI wykonywane przez kierownictwo
- ❖ uaktualnianie planów bezpieczeństwa
- ❖ rejestrowanie działań i zdarzeń mogących mieć wpływ na wydajność działania SZBI



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



4.2.4 UTRZYMYWANIE I DOSKONALENIE SZBI

- ❖ wdrażanie zidentyfikowanych w SZBI udoskonaleń
- ❖ podejmowanie odpowiednich działań korygujących i/lub zapobiegawczych
- ❖ informowanie zainteresowanych stron o działaniach i udoskonaleniach
- ❖ zapewnienie, że udoskonalenia osiągają zamierzone cele



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



4.3.1 WYMAGANIA DOTYCZĄCE DOKUMENTACJI

Dokumentacja SZBI powinna obejmować:

- ❖ deklaracje polityki SZBI
- ❖ zakres SZBI
- ❖ procedury i zabezpieczenia wspomagające SZBI
- ❖ opis metodyki szacowania ryzyka



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



4.3.1 WYMAGANIA DOTYCZĄCE DOKUMENTACJI

- ❖ raport z procesu szacowania ryzyka
- ❖ plan postępowania z ryzykiem
- ❖ deklarację stosowania
- ❖ zapisy wymagane normą PN-ISO/IEC 27001
- ❖ inne procedury



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



4.3.2 NADZÓR NAD DOKUMENTAMI

4.3.3 NADZÓR NAD ZAPISAMI

Należy ustanowić procedury dotyczące nadzoru nad dokumentami i zapisami

Dokumenty powinny być:

- ❖ możliwe do zlokalizowania
- ❖ poddawane okresowym przeglądom
- ❖ dostępne w aktualnej wersji
- ❖ nieaktualne bezzwłocznie usuwane lub przechowywane



4.3.2 NADZÓR NAD DOKUMENTAMI

4.3.3 NADZÓR NAD ZAPISAMI

Zapisy powinny :

- ❖ być łatwo dostępne
- ❖ być możliwe do zidentyfikowania
- ❖ mieć czasokres przechowywania
- ❖ być zabezpieczone przed zniszczeniem
- ❖ być czytelne
- ❖ być zrozumiałe



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



5. ODPOWIEDZIALNOŚĆ KIEROWNICTWA

5.1 Zaangażowanie kierownictwa

- ❖ ustanowienie polityki bezpieczeństwa informacji
- ❖ zapewnienie, że cele i plany bezpieczeństwa informacji są ustanowione
- ❖ ustalenie zadań i odpowiedzialności dla bezpieczeństwa informacji
- ❖ zakomunikowanie wagi spełnienia wypełnienia celów zgodnych z polityką bezpieczeństwa informacji
- ❖ zapewnienia niezbędnych zasobów
- ❖ zatwierdzenie akceptowalnego poziomu ryzyka
- ❖ przeprowadzenie przeglądów zarządzania

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



5.2 ZARZĄDZANIE ZASOBAMI

5.2.1 Zapewnienie zasobów

- ❖ ustanowienia, wdrożenia, funkcjonowania i doskonalenia
- ❖ weryfikacji czy procedury bezpieczeństwa informacji wspierają wymagania biznesowe
- ❖ spełnienia wymogów prawnych
- ❖ utrzymanie odpowiedniego poziomu bezpieczeństwa przez zastosowanie wdrożonych zabezpieczeń
- ❖ prowadzenie przeglądów SZBI
- ❖ gdy potrzeba – podnoszenie skuteczności systemu

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



5.2.2 SZKOLENIA, UŚWIADAMIANIE I KOMPETENCJE

- ❖ określenie koniecznych kompetencji personelu
- ❖ zapewnienie szkoleń w celu realizacji potrzeb
- ❖ ocena skuteczności szkoleń oraz podjętych działań
- ❖ prowadzenie zapisów dotyczących szkoleń
- ❖ uświadamianie związku i znaczenia personelu w SZBI



6. WEWNĘTRZNE AUDITY SZBI

Określenie, czy cele stosowania zabezpieczeń, zabezpieczenia, procesy i procedury SZBI są:

- ❖ zgodne z wymaganiami normy
- ❖ zgodne ze zidentyfikowanymi wymaganiami bezpieczeństwa informacji
- ❖ skutecznie wdrożone i utrzymywane
- ❖ zgodne z oczekiwaniami



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



6. WEWNĘTRZNE AUDITY SZBI

- ❖ polityka bezpieczeństwa jest aktualna i spełnia wymagania biznesowe
- ❖ metodyka zarządzania ryzykiem jest odpowiednia
- ❖ udokumentowane procedury ISMS spełniają zamierzone cele i są przestrzegane

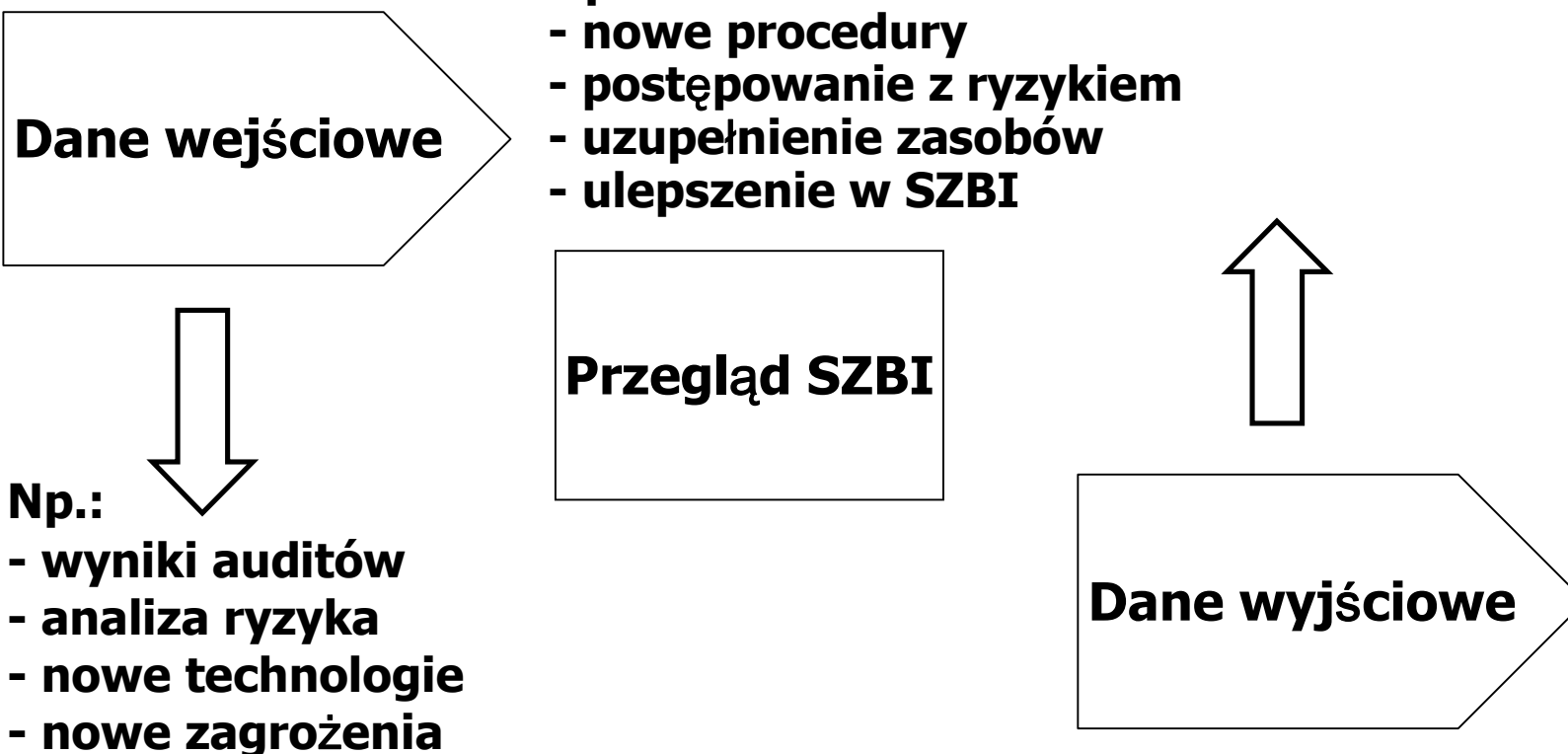


6. WEWNĘTRZNE AUDITY SZBI

- ❖ zabezpieczenia techniczne są poprawnie zaimplementowane, skonfigurowane i działają zgodnie z zamierzeniami
- ❖ ryzyka szczątkowe są odpowiednio oszacowane i zaakceptowane przez kierownictwo
- ❖ rekomendacje wynikające z poprzednich audytów zostały zrealizowane
- ❖ SZBI spełnia wymagania normy PN-ISO/IEC 27001



7. PRZEGLĄDY SZBI REALIZOWANE PRZEZ KIEROWNICTWO

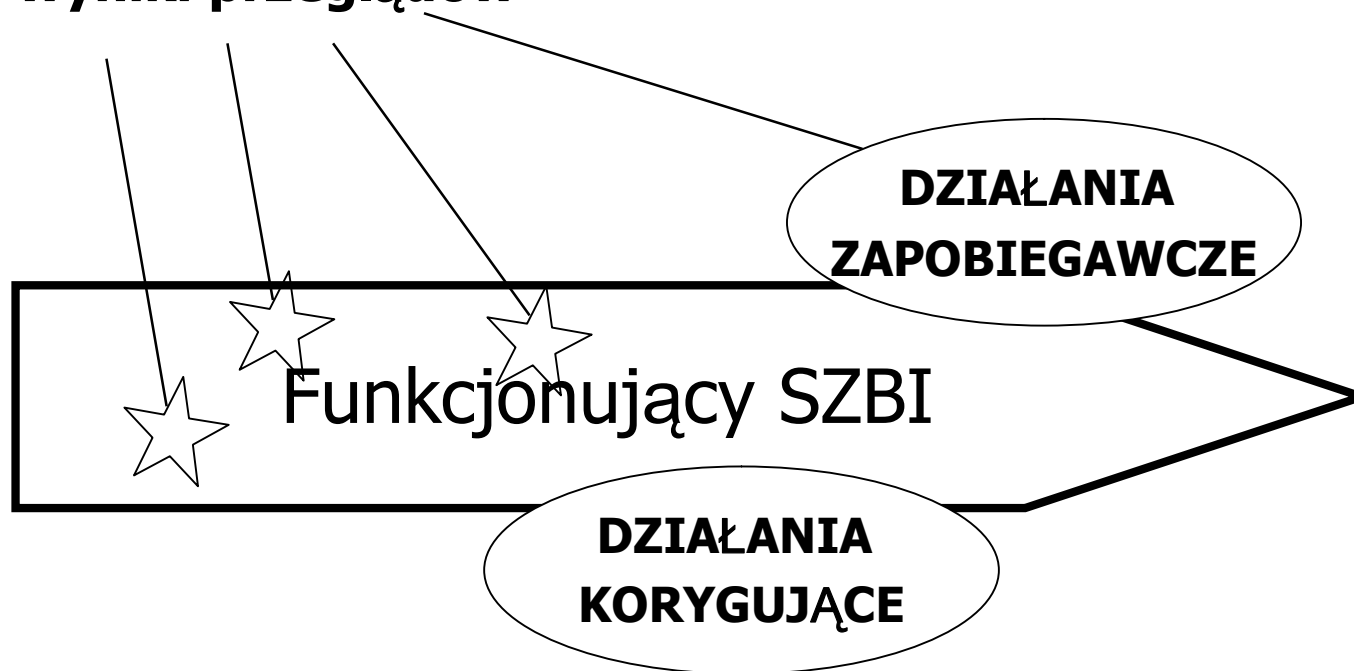




8. DOSKONALENIE SZBI

Np.:

- ❖ **zagrożenia**
- ❖ **wyniki przeglądów**





KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



ZAŁĄCZNIK A DO NORMY PN-ISO/IEC 27001

5. polityka bezpieczeństwa informacji
6. Organizacja bezpieczeństwa informacji
7. Zarządzanie aktywami
8. Bezpieczeństwo osobowe
9. Bezpieczeństwo fizyczne i środowiskowe
10. Zarządzanie działalnością oraz komunikacją
11. Kontrola dostępu
12. Zbieranie danych, rozwój oraz utrzymanie systemu
13. Zarządzanie incydentami bezpieczeństwa informacji
14. Zarządzanie ciągłością działania
15. Zgodność

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



DZIĘKUJĘ ZA UWAGĘ

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego