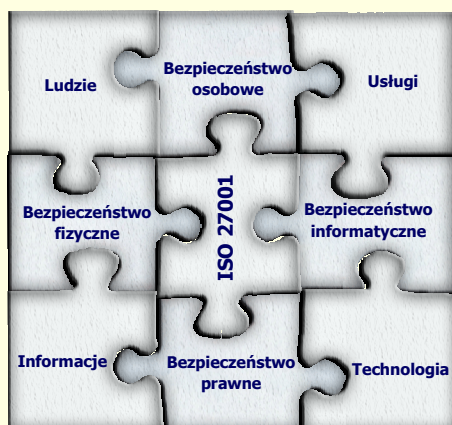


CONFIDENCE 2007

Analiza ryzyka podstawą wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z ISO/IEC 27001:2005

Krzysztof Maćkowiak
Doradztwo Gospodarcze DGA SA

Systemowe podejście do bezpieczeństwa informacji



Doradztwo Gospodarcze DGA SA

ISO/IEC 27001:2005 a ISO/IEC 17799:2005

Norma ISO/IEC 27001 służy do certyfikacji

Norma ISO/IEC 17799 – jest kodeksem, zawiera wytyczne, a nie wymagania

Wymagania

Wytyczne

System zarządzania bezpieczeństwem informacji

Doradztwo Gospodarcze DGA SA

Historia standardów



Standardy:

- Polskie
- Brytyjskie
- Międzynarodowe

1993

BS PD0003:1993

WYTYCZNE

WYMAGANIA

1995

BS 7799-1:1995

1998

BS 7799-2:1998

1999

BS 7799-1:1999

BS 7799-2:1999

2000

ISO/IEC 17799:2000

2002

BS 7799-1:2002

BS 7799-2:2002

2003

PN-ISO 17799:2003

2005

ISO/IEC 17799:2005

PN-1-07799-2:2005

ISO/IEC 27001:2005

2007

Rodzina standardów ISO/IEC 27000

Doradztwo Gospodarcze DGA SA

Budowa normy ISO/IEC 27001:2005

Wymagania

- 0 Wstęp
- 1 Zakres normy
- 2 Odwołania normatywne
- 3 Terminy i definicje
- 4 System zarządzania bezpieczeństwem informacji
- 5 Odpowiedzialność kierownictwa
- 6 Audyty wewnętrzne
- 7 Przegląd kierownictwa SZBI
- 8 Udoskonalanie SZBI
- 9 Załącznik A

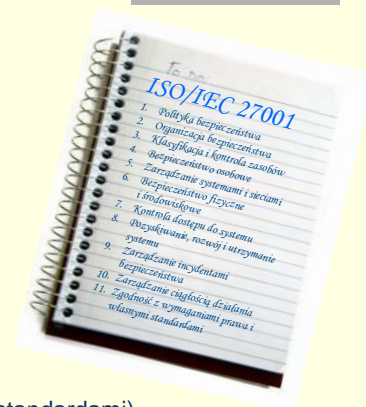


Doradztwo Gospodarcze DGA SA

Budowa normy ISO/IEC 27001:2005

Wymagania

- A.5 Polityka bezpieczeństwa
- A.6 Organizacja bezpieczeństwa informacji
- A.7 Zarządzanie aktywami
- A.8 Bezpieczeństwo osobowe
- A.9 Bezpieczeństwo fizyczne i środowiskowe
- A.10 Zarządzanie systemami i sieciami
- A.11 Kontrola dostępu do systemów
- A.12 Pozyskanie, rozwój i utrzymanie systemów
- A.13 Zarządzanie incydentami bezpieczeństwa
- A.14 Zarządzanie ciągłością działania
- A.15 Zgodność (z wymaganiami prawa i własnymi standardami)



Doradztwo Gospodarcze DGA SA

Zarządzanie bezpieczeństwem informacji – podejście procesowe

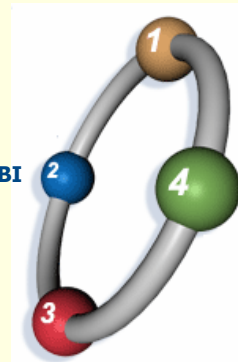
Głównym celem SZBI jest minimalizacja ryzyka utraty najważniejszych informacji organizacji

Wdrożenie i eksploatacja SZBI

Monitorowanie i przegląd SZBI

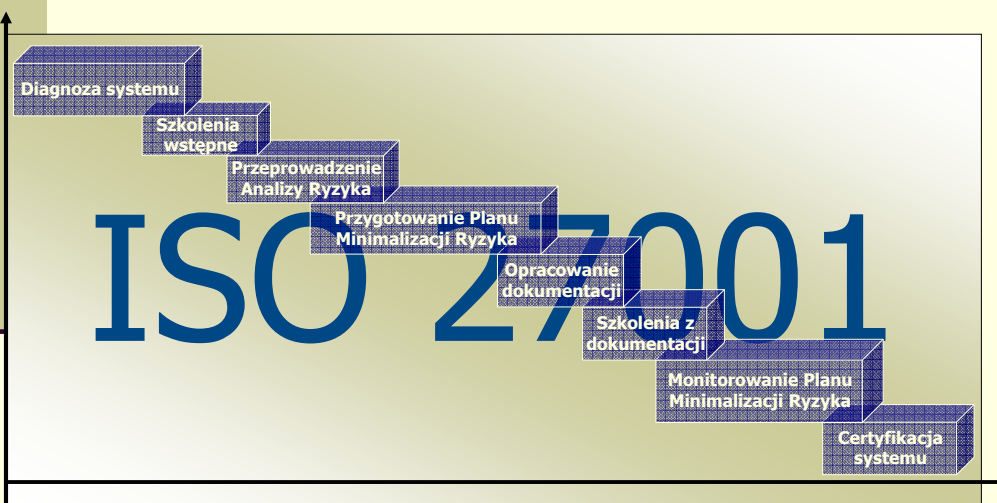
Ustanowienie SZBI

Utrzymanie i doskonalenie SZBI



Doradztwo Gospodarcze DGA SA

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji

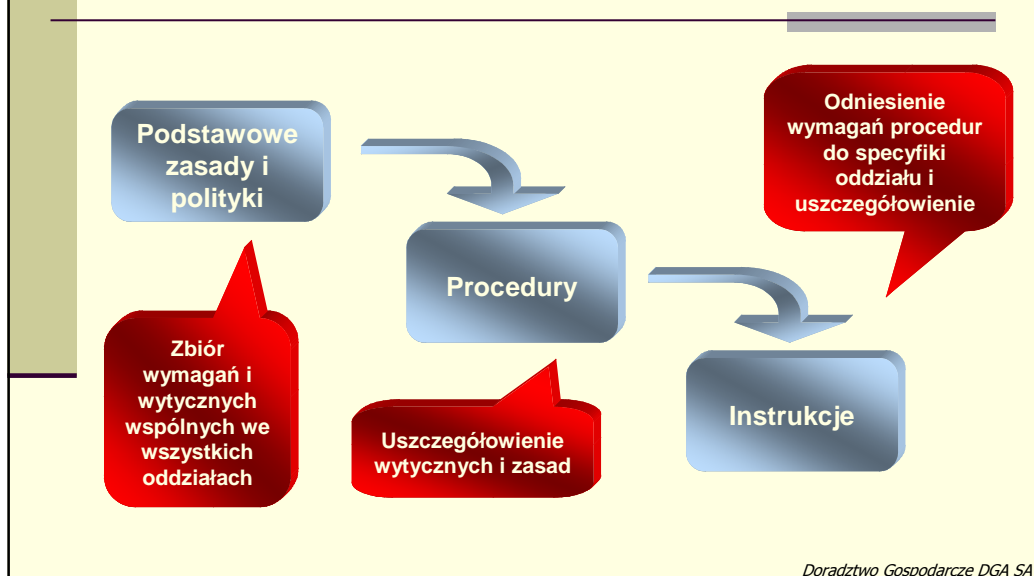


Doradztwo Gospodarcze DGA SA

Ogólny model zarządzania bezpieczeństwem informacji



Hierarchiczna struktura dokumentacji SZBI



Zarządzanie ryzykiem – podstawowe terminy

Zasoby/aktywa – wszystkie elementy systemu, które mają wartość dla organizacji – np. informacje, systemy informatyczne, sprzęt, budynki, ludzie itp.



Doradztwo Gospodarcze DGA SA

Zarządzanie ryzykiem – podstawowe terminy

Zagrożenie – potencjalna przyczyna niepożądanego zdarzenia, który może wpłynąć na zasób np. kradzież, pożar, powódź, włamanie do systemu, wirus komputerowy.



Doradztwo Gospodarcze DGA SA

Zarządzanie ryzykiem – podstawowe terminy

Podatność – słabość zasobu lub grupy zasobów, która może być wykorzystana przez jedno lub więcej zagrożeń, np. brak hasła, brak szyfrowania danych, brak zamków w szafie, niezamykane pomieszczenia.



Doradztwo Gospodarcze DGA SA

Zarządzanie ryzykiem – podstawowe terminy

Zagrożenia

- Kradzież informacji
- Awaria sprzętu
- Atak wirusowy
- Błąd ludzki
- Zniszczenie dokumentów
- Włamanie do systemu informatycznego



Podatności

- Brak zabezpieczeń fizycznych
- Brak klimatyzacji w serwerowni
- Brak ochrony antywirusowej
- Brak szkoleń dla pracowników
- Rura z wodą w archiwum
- Brak haseł w systemie informatycznym

Doradztwo Gospodarcze DGA SA

Zarządzanie ryzykiem – podstawowe terminy

Ryzyko - prawdopodobieństwo tego, że określone zagrożenie wykorzysta podatność aktywu lub grupy aktywów w celu spowodowania strat lub zniszczenia aktywów

Doradztwo Gospodarcze DGA SA

Zarządzanie ryzykiem – podstawowe terminy

Pamiętajmy jeszcze o skutkach utraty (następstwach)

Doradztwo Gospodarcze DGA SA

Zarządzanie ryzykiem

Analiza ryzyka – metoda systematycznej identyfikacji zasobów systemu przetwarzania danych, zagrożeń dla tych zasobów i podatności systemu na te zagrożenia

Zarządzanie ryzykiem - całkowity proces identyfikacji, kontrolowania i eliminacji (lub minimalizowania) prawdopodobieństwa zaistnienia niepewnych zdarzeń mogących mieć wpływ na zasoby systemu informacyjnego

Metody postępowanie z ryzykiem:

Akceptacja ryzyka – decyzja kierownictwa dopuszczająca pewien stopień ryzyka, zwykle z przyczyn technicznych lub finansowych

Redukcja ryzyka – wdrożenie zabezpieczeń zmniejszających ryzyko

Transfer ryzyka – ubezpieczenie (minimalizacja następstw)

Unikanie ryzyka – np. wycofanie usługi

Doradztwo Gospodarcze DGA SA

Podział metod analizy ryzyka

Metody ilościowe

- Bazują na obliczeniach matematycznych i obiektywnej ocenie.
- Wymagają szczegółowych danych liczbowych dotyczących zagrożeń, podatności i prawdopodobieństwa.
- Pozwalają na uzyskanie stosunkowo dokładnych i precyzyjnych wniosków dotyczących zwiększenia bezpieczeństwa.

Ryzyko: 1,2,3, 2.43, 4.34

Metody jakościowe

- Polegają tylko na subiektywnej ocenie, nie posługują się wyliczeniami.
- Pozwalają tylko na hierarchiczne uporządkowanie ryzyk.
- Mogą być mało dokładne, dlatego niezbędny jest ciągły nadzór nad procesem analizy ryzyka i duża wiedza merytoryczna osób ją przeprowadzających.

Ryzyko: niskie, średni, wysokie, większe niż ..., mniejsze niż...

Doradztwo Gospodarcze DGA SA

Podział metod analizy ryzyka



- **Ilościowe metody analizy ryzyka**
 - Oczekiwana roczna strata
 - Drzewa zdarzeń (ETA)
 - Drzewa błędów (FTA)
- **Jakościowe metody analizy ryzyka**
 - Drzewa zdarzeń (ETA)
 - Drzewa błędów (FTA)
 - Wstępna analiza ryzyka (PRA – Preliminary Risk Analysis)
 - HAZOP
 - Analiza defektów (FMEA, FMECA)

Doradztwo Gospodarcze DGA SA

Ilościowe metody analizy ryzyka



Oczekiwana roczna strata

Najprostsza kosztowa metoda analizy ryzyka

- Ryzyko wyrażane przez współczynnik oczekiwanej rocznej straty (ALE - Annual Loss Exposure / Expectancy):

$$\text{ALE} = P \times S$$

gdzie:

P – prawdopodobieństwo wykorzystania określonej podatności przez dane zagrożenie w celu spowodowania straty,

S – wartość zasobu (skutek utraty).

Doradztwo Gospodarcze DGA SA

Ilościowe metody analizy ryzyka

Drzewa zdarzeń (ETA – Event Tree Analysis)

- Graficzna metoda prezentacji procesu analizy ryzyka.
- Obrazuje zależności przyczynowo – skutkowe.
- Charakter indukcyjny – na podstawie zdarzenia cząstkowego wnioskuje się wszystkie możliwe skutki.
- Drzewo zdarzeń rozpoczyna się zdarzeniem inicjującym. Kolejne rozgałęzienie przedstawiają wszystkie możliwe ciągi zdarzeń będące następstwami zdarzenia inicjującego.
- Prawdopodobieństwo wystąpienia określonego skutku otrzymujemy mnożąc prawdopodobieństwa wszystkich zdarzeń składających się na gałąź, po której dochodzimy do danego skutku.
- Metoda może być rozpatrywana również jako metoda ilościowa (brak określonych współczynników prawdopodobieństwa).

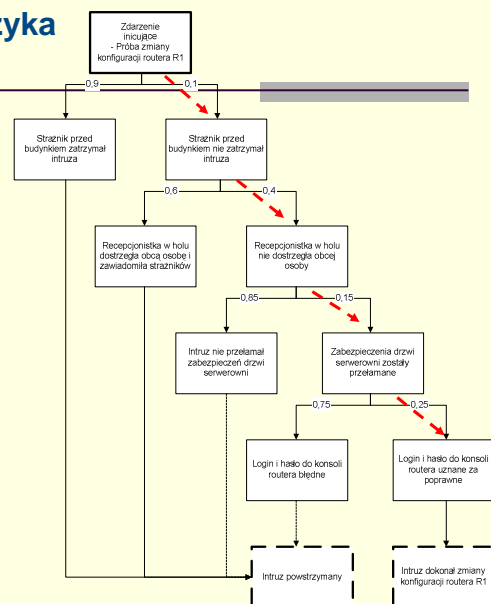


Doradztwo Gospodarcze DGA SA

Ilościowe metody analizy ryzyka

Drzewa zdarzeń

$$P = 0,1 \times 0,4 \times 0,15 \times 0,25 = 0,0015$$



Doradztwo Gospodarcze DGA SA

Ilościowe metody analizy ryzyka

Drzewa błędów (FTA – Fault Tree Analysis)

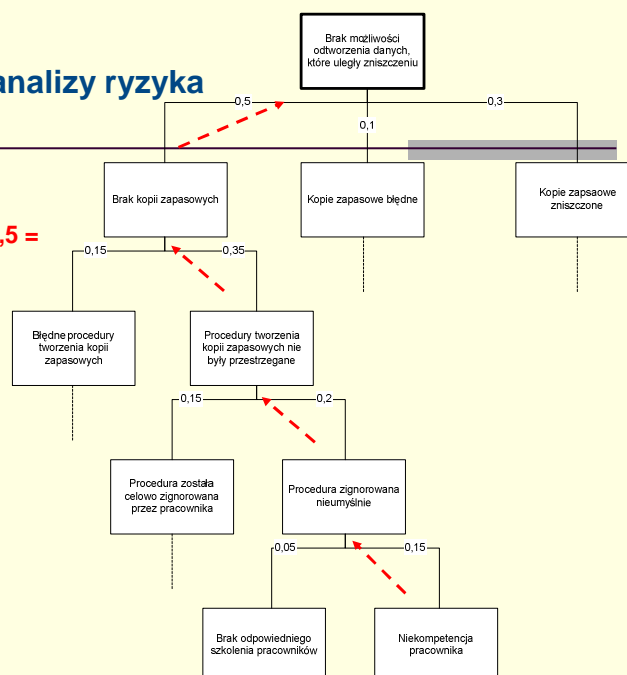
- Opracowana w Bell Telephone Laboratories podczas prac nad międzykontynentalnymi pociskami balistycznymi.
- Graficzna metoda prezentacji procesu analizy ryzyka.
- Obrazuje zależności przyczynowo – skutkowe.
- Budowane w przeciwnym kierunku niż drzewo zdarzeń.
- Na początku (u góry schematu) przedstawiony zostaje określony skutek, a analiza drzewa w dół pozwala na określenie przyczyn.
- Metoda może być rozpatrywana również jako metoda ilościowa (brak określonych współczynników prawdopodobieństwa).

Doradztwo Gospodarcze DGA SA

Ilościowe metody analizy ryzyka

Drzewa błędów

$$P = 0,15 \times 0,2 \times 0,35 \times 0,5 = 0,00525$$



Doradztwo Gospodarcze DGA SA

Zarządzanie ryzykiem – wymagania ISO/IEC 27001:2005

- Zdefiniować systematyczne podejście do analizy ryzyka
- Identyfikować ryzyka
 - Przeprowadzić inwentaryzację (klasyfikację) zasobów
 - Określić zagrożenia dla zdefiniowanych zasobów
 - Zidentyfikować słabości, które mogą zostać wykorzystane przez zagrożenia
 - Oszacować skutki zrealizowania się zagrożeń w odniesieniu do utraty poufności, integralności lub dostępności zasobów
- Wyznaczyć ryzyko
 - Określić skutki wystąpienia zagrożenia jako miarę kosztów zastąpienia lub odnowienia zasobu
 - Określić prawdopodobieństwo wystąpienia zagrożenia, przy uwzględnieniu środków kontroli już wprowadzonych
 - Oszacować ryzyko utraty informacji
 - Oszacować, czy ryzyko jest akceptowalne, czy wymaga podjęcia działań dla jego zmniejszenia

Doradztwo Gospodarcze DGA SA

Problemy na etapie wdrażania SZBI

- Brak wiedzy merytorycznej
- Brak wyznaczonych osób (grupy roboczej) oraz określonych odpowiedzialności w zakresie realizacji działań stanowiących wdrożenie SZBI
- Brak wsparcia kierownictwa
- Brak zasobów ludzkich/finansowych
- Brak zainteresowania/zrozumienia wśród pracowników



Doradztwo Gospodarcze DGA SA

Problemy na etapie funkcjonowania SZBI

- Błędne zarządzanie incydentami – gdy incydenty stanowią podstawę do karania pracowników
- Brak aktywności użytkowników (zgłaszanie incydentów, słabości, zmian do dokumentacji)
- Brak znajomości zasad SZBI = brak stosowania tych zasad
- Brak działań mających na celu utrzymanie skuteczności systemu (problemy w czasie audytu nadzoru)
- Brak szkoleń dla nowych pracowników
- Nieaktualna dokumentacji



Doradztwo Gospodarcze DGA SA

CONFIDENCE 2007

Dziękuję za uwagę i zapraszam



www.Centrum.Bezpieczenstwa.pl



www.kryptografia.com