

Analiza i zarządzanie ryzykiem związane z eksploatacją systemów informacyjnych w świetle obowiązujących ustaw i norm

Imed El Fray

Włodzimierz Chocianowicz

Laboratorium Certyfikacji Produktów i Systemów Informatycznych

Wydział Informatyki

Katedra Inżynierii Oprogramowania

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

(dawniej Politechnika Szczecińska)



Zachodniopomorski
Uniwersytet
Technologiczny
w Szczecinie

Informacja i jej formy

- **Informacje to aktywa**, które podobnie jak inne ważne aktywa biznesowe, są niezbędne do działalności biznesowej organizacji i z tego powodu zaleca się ich odpowiednią ochronę (PN ISO/IEC 17799:2007)
 - **Aktywa** - wszystko, co ma wartość dla organizacji (PN ISO/IEC 13335-1)
- Informacja może przybierać różne formy:
 - może być wydrukowana lub zapisana odręcznie na papierze,
 - może być przechowywana elektronicznie, przesyłana pocztą lub za pomocą urządzeń elektronicznych,
 - może być wyświetlana w formie filmów lub wypowiedzana w czasie rozmowy.
- Zawsze musi być jednak w odpowiedni sposób chroniona!

Dane osobowe i informacja niejawna

- Problemy ochrony danych osobowych i informacji niejawnej regulowane są przez następujące Ustawy:
 - Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, Nr 182, poz.1228)
 - Ustawa dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U z 2002 r. Nr 101, poz. 926, z późn. zm.)
- ... oraz dziesiątki towarzyszących im rozporządzeń i zarządzeń!

Ustawa o ochronie informacji niejawnych

- Art.1, ust.2 Przepisy ustawy mają zastosowanie do:
 - 1) organów władzy publicznej, w szczególności:
 - c) organów administracji rządowej,
 - d) organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych,
- Art.2. W rozumieniu ustawy:
 - 15) ryzykiem – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji.
 - 16) szacowaniem ryzyka – jest całościowy proces analizy i oceny ryzyka.
 - 17) zarządzaniem ryzykiem – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka,

Ustawa o ochronie informacji niejawnych

- Art.15,ust.1. Do zadań pełnomocnika ochrony należy:
 - 3) **zarządzanie ryzykiem** bezpieczeństwa informacji niejawnych, w szczególności **szacowanie ryzyka**;
- Art.19,ust.1. 1. Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu zapoznania z:
 - 2) zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad **zarządzania ryzykiem** bezpieczeństwa informacji niejawnych, w szczególności **szacowania ryzyka**;

Ustawa o ochronie informacji niejawnych

- Art.49, ust.1. **Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego** powinien zawierać w szczególności wyniki procesu **szacowania ryzyka** dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach **zarządzania ryzykiem** sposoby osiągnięcia i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo. Przebieg i wyniki procesu **szacowania ryzyka** mogą zostać przedstawione w odrębnym dokumencie niż dokument szczególnych wymagań bezpieczeństwa.

Ustawa o ochronie informacji niejawnych

- Art.49, ust.4. **Podstawą dokonywania wszelkich zmian w systemie teleinformatycznym** jest przeprowadzenie procesu **szacowania ryzyka** dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.
- Art.49, ust.7. Kierownik jednostki organizacyjnej akceptuje wyniki procesu **szacowania ryzyka** dla bezpieczeństwa informacji niejawnych oraz jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego.
 - Art.49, ust.9. Prezes Rady Ministrów określi, w drodze rozporządzenia, podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne, niezbędne dane, jakie powinna zawierać dokumentacja bezpieczeństwa systemów informatycznych oraz sposób opracowania tej dokumentacji.
 - Art.49, ust.10. W rozporządzeniu, o którym mowa w ust. 9, Prezes Rady Ministrów uwzględni w szczególności wymagania w zakresie zarządzania ryzykiem oraz dotyczące zapewnienia poufności, integralności i dostępności informacji niejawnych przetwarzanych w systemach teleinformatycznych.

**ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW**

z dnia

w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

Rozdział 2

Podstawowe wymagania bezpieczeństwa teleinformatycznego

- § 5. 1. Bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym zapewnia się przez wdrożenie spójnego zbioru zabezpieczeń w celu zapewnienia poufności, integralności i dostępności tych informacji.
2. Cel, o którym mowa w ust. 1, osiąga się poprzez:
- 1) objęcie systemu teleinformatycznego **procesem zarządzania ryzykiem** dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym, zwanego dalej „zarządzaniem ryzykiem w systemie teleinformatycznym”;

**ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW**

z dnia

w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

Rozdział 4

Dokumentacja bezpieczeństwa teleinformatycznego

§ 26. 1. W dokumencie procedur bezpiecznej eksploatacji określa się szczegółowy wykaz procedur bezpieczeństwa wraz z dokładnym opisem sposobu ich wykonania, realizowanych przez osoby odpowiedzialne za bezpieczeństwo teleinformatyczne oraz osoby uprawnione do pracy w systemie teleinformatycznym, obejmujący:

- 1) administrowanie systemem teleinformatycznym oraz zastosowanymi środkami zabezpieczającymi;
- 2) bezpieczeństwo urządzeń;
- 3) bezpieczeństwo oprogramowania;
- 4) zarządzanie konfiguracją sprzętowo-programową, w tym zasady serwisowania lub modernizacji oraz wycofywania z użycia elementów systemu teleinformatycznego;
- 5) plany awaryjne;
- 6) monitorowanie i **audyt** systemu teleinformatycznego;
- 7) zarządzanie nośnikami;
- 8) zarządzanie materiałami kryptograficznymi;
- 9) stosowanie ochrony elektromagnetycznej;...

Ochrona danych osobowych - rozporządzenia i normy

- Rozporządzenie Prezesa RM z dn. 25.02.1999 w sprawie *podstawowych wymagań bezpieczeństwa systemów i sieci TI* (Dz.U. Nr 18, poz.162)
- Rozporządzenie MSWiA z dnia 3 czerwca 1998 r. w sprawie *określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz. U. Nr 80, poz.521)
- PN-I-13335 -1:1999 Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych

Ochrona danych osobowych

- Ustawa o ochronie danych osobowych określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych.
- Organem do spraw ochrony danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych.
- Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą.
- Administrator danych wyznacza osobę, zwaną **administratorem bezpieczeństwa informacji**

PN-I-02000:2002

Technika informatyczna – Zabezpieczenia w systemach informatycznych --Terminologia

PN-ISO/IEC 2382-8:2001

Technika informatyczna -- Terminologia -- Bezpieczeństwo

- **bezpieczeństwo systemu informatycznego**

ochrona danych i zasobów przed przypadkowymi lub złośliwymi czynami, polegająca zwykle na podjęciu właściwych działań

UWAGA - Tymi czynami mogą być: modyfikacja, zniszczenie, dostęp, ujawnienie lub pozyskanie danych, gdy (**czyny te**) są nieuprawnione albo następuje ich (**danych**) strata

- **ryzyko**

możliwość, że konkretne **zagrożenie** wykorzysta konkretną **podatność** systemu przetwarzania danych

- **zagrożenie**

potencjalna możliwość naruszenia **bezpieczeństwa systemu informatycznego**

- **podatność**¹

słabość lub luka w systemie przetwarzania danych

PN-I-02000:2002

Technika informatyczna – Zabezpieczenia w systemach informatycznych --Terminologia

PN-ISO/IEC 2382-8:2001

Technika informatyczna -- Terminologia -- Bezpieczeństwo

- **podatność**²

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

- **analiza ryzyka, szacowanie ryzyka**

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

- **zarządzanie ryzykiem**

element teorii zarządzania dotyczący identyfikacji, pomiaru, nadzoru i minimalizacji możliwości wystąpienia zdarzeń niepewnych, który zawiera skuteczny program zarządzania obejmujący ocenę **ryzyka**, określaną na podstawie oceny **zagrożeń** i **podatności**, decyzje zarządzające, wdrożenie środków kontroli i przegląd **skuteczności**

PN-I-02000:2002

Technika informatyczna – Zabezpieczenia w systemach informatycznych --Terminologia

PN-ISO/IEC 2382-8:2001

Technika informatyczna -- Terminologia -- Bezpieczeństwo

- **audyt bezpieczeństwa**

niezależny przegląd i sprawdzenie zapisów oraz funkcji systemu przetwarzania danych w celu sprawdzenia prawidłowości kontroli systemowej, zapewnienia zgodności z przyjętą **polityką bezpieczeństwa** i procedurami działania, w celu wykrycia przełamań bezpieczeństwa oraz w celu zalecenia określonych zmian w kontroli, polityce bezpieczeństwa i procedurach

- **polityka bezpieczeństwa** ¹

plan lub sposób postępowania przyjęty w celu zapewnienia **bezpieczeństwa systemu informatycznego**

- **polityka bezpieczeństwa** ²

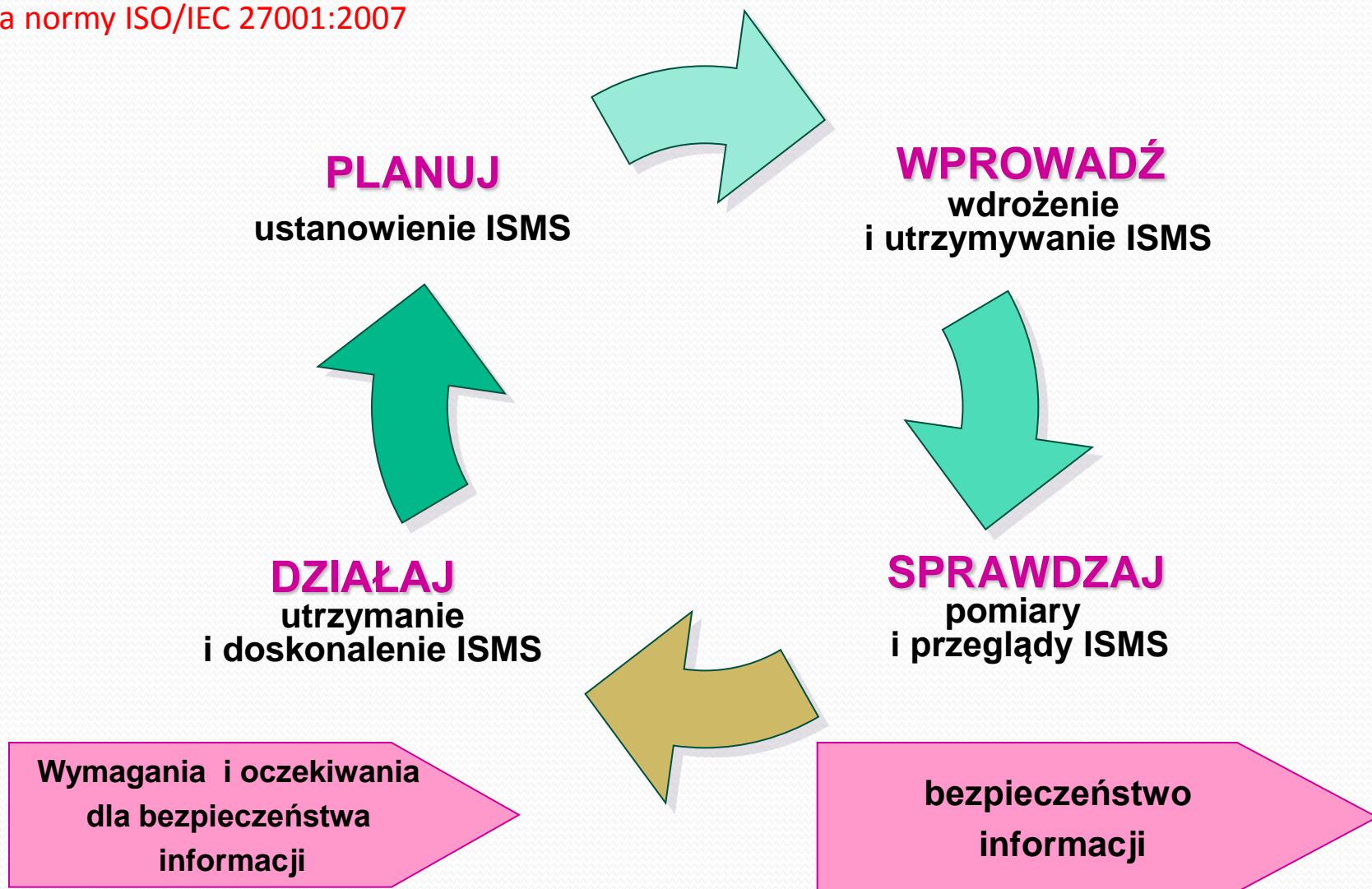
zestaw reguł określających wykorzystanie informacji, łącznie z jej przetwarzaniem, przechowywaniem, dystrybucją i prezentacją, niezależnie od wymagań dotyczących bezpieczeństwa i celów bezpieczeństwa

System zarządzania bezpieczeństwem informacji (ISMS - ZBSI)

- **System zarządzania bezpieczeństwem informacji** - część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do **ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia** bezpieczeństwa informacji
 - System zarządzania obejmuje strukturę organizacyjną, polityki, zaplanowane działania, zakresy odpowiedzialności, praktyki, procedury, procesy i zasoby.
- Podstawowe normy
 - PN ISO/IEC 17799:2005 *Praktyczne zasady zarządzania bezpieczeństwem informacji*, PKN, 2007
 - PN ISO/IEC 27001:2007 *Systemy zarządzania bezpieczeństwem informacji*, PKN, 2007

Wymagania normy ISO 27001:2007

Budowa normy ISO/IEC 27001:2007



Proces Zarządzania Bezpieczeństwem SI?

■ ZBSI jest procesem, którego celem jest:

- ✓ określanie strategii bezpieczeństwa organizacji,
- ✓ zidentyfikowanie i klasyfikacja zasobów,
- ✓ zidentyfikowanie i zanalizowanie zagrożeń i podatności systemu,
- ✓ zidentyfikowanie i przeanalizowanie ryzyka,



Wiedzieć co realnie zagraża systemowi

- ✓ określenie odpowiednich zabezpieczeń,



Odpowiednio zabezpieczyć system

- ✓ monitorowanie procesu wdrożenia i działania zabezpieczeń,

- ✓ opracowanie i wdrażanie programu uświadamiania dot. bezpieczeństwa oraz wykrywanie incydentów i reagowanie na nie.



Utrzymywanie przyjętego poziomu bezpieczeństwa

Proces Zarządzania Ryzykiem

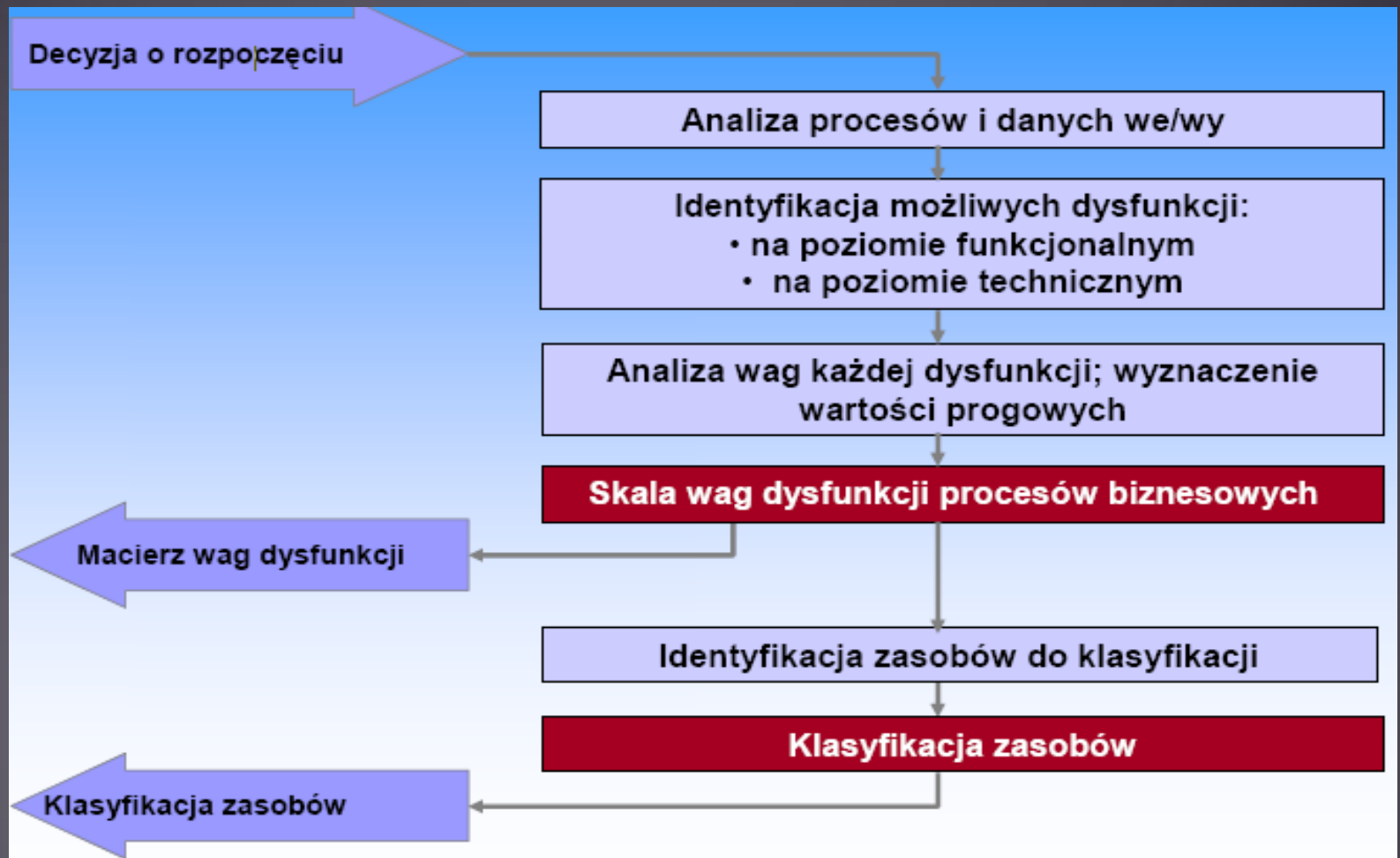


Model Analizy Ryzyka



Analiza ryzyka – etap I - klasyfikacja zasobów

Proces



Analiza i klasyfikacja zasobów i informacji

Tworzona macierz zasobów

Macierz skutku właściwego				
Klasyfikacje danych, informacji i elementy infrastruktury informatycznej i telekomunikacyjnej				
Dane i informacji		D	I	P
D01	Pliki danych lub bazy danych	2	2	3
D02	Pliki biurowe przechowywane na serwerze z dostępem współdzielonym	3	2	2
D03	Pliki biurowe przechowywane w komputerach osobistych	2	1	3
D04	Zapiski odręczne lub wydruki przechowywane przez użytkowników	2		2
D05	Listingi lub wydruki (np. z aplikacji informatycznych)			3
D06	Informacje, dane lub wiadomości wymieniane, wysyłane itp.	3	3	2
D07	Poczta i faksy	2	3	2
D08	Archiwa mające wartość dowodową (np. KRS, REGON, Akcenariusze itp.)	2		
D09	Dane i informacje publikowane na stronach WWW	3	3	1
Infrastruktura informatyczna i telekomunikacyjna		D	I	P
R01	Okablowanie, sprzęt i oprogramowanie sieciowe WAN	2	2	
R02	Okablowanie, sprzęt i oprogramowanie sieciowe LAN	2	3	
R03	Dane konfiguracyjne sieci WAN	2	3	4
R04	Dane konfiguracyjne sieci LAN	3	3	4
S01	serwery plików współdzielonych itp.)	2	2	
S02	Pliki konfiguracyjne dla serwerów i systemów głównych	3	4	2
S03	Terminale i konsole na potrzeby użytkowników (drukarki lokalne, interfejsy itp.)	2		
A01	Oprogramowanie (wersje wykonywalna)	1	2	2
A02	Kody źródłowe dla oprogramowania	4	3	2
A03	Pliki konfiguracyjne dla aplikacji (oprogramowania)	3	4	3
A04	Dedykowane oprogramowania i aplikacje	1		
Infrastruktura lokalna				
E01	Miejsce i otoczenie pracy (np. biura itp.)	2		
E02	Łącza telekomunikacyjne (głosowe i analogowe)	2	3	
I01	komputerowe itp..	3		
Skutek właściwy nie zależny od klasyfikacji zasobów i informacji				
Niedostępność personelu				
P01	Personel specjalistyczny (administratorzy, projektanci itp.)	2		
P02	Użytkownicy	3		
Niezgodność z prawem i ustawami				
C01	Niezgodność z prawem i regulacjami prawnymi (np. Ustawami) odnośnie ochrony życia i prywatności personelu	2		
C02	Niezgodność z prawem i regulacjami prawnymi (np. Ustawami) odnośnie kontroli finansowej	2		
C03	Niezgodność z prawem i regulacjami prawnymi (np. Ustawami) odnośnie własności intelektualnej	3		
C04	Niezgodność z prawem i regulacjami prawnymi (np. Ustawami) odnośnie ochrony systemów informatycznych	3		
C05	Niezgodność z regulaminami prawnymi odnośnie bezpieczeństwa personelu i ochrony środowiska	2		

Etap II - Identyfikacja podatności zasobów

Przykład macierz podatności

Oszacowanie podatności		P=1	P=2	P=3	P=4
Oszacowanie prawdopodobieństwa zdarzeń		Bardzo niskie	Niskie	możliwe	Bardzo możliwe
Wypadki / Zdarzenia losowe					
AC01	Zwarcie na poziomie okablowania lub urządzenia		X		
AC06	Zalanie spowodowane wylaniem rzeki lub wystąpieniem wód gruntowych		X		
AC09	Całkowita niedostępność pomieszczeń: zakaz dostępu (ryzyko zanieczyszczenia, zamieszki, itp.) wydany przez specjalistyczną jednostkę (np. Straż pożarna, Policja lub Prefektura)		X		
AC14	Blokada aplikacji lub systemu niemożliwa do usunięcia przez serwis z powodu zniknięcia głównego specjalisty lub dostawcy		X		
AC17	Wymazywanie danych lub konfiguracji spowodowane wirusem			X	
AC19	Przypadkowa utrata plików danych w wyniku starzenia lub zanieczyszczenia nośnika		X		
Działania Celowe					
MA06	Samowolne skasowanie (bezpośrednie lub pośrednie) oprogramowania (np. przechowywanego na nośniku itp.)		X		
MA08	Manipulacja danych lub podanie fałszywych danych na wejściu			X	
MA09	Dostęp do wrażliwych danych współdzielonych i ich ujawnienie			X	
MA10	Przechwycenie plików i/lub kradzież nośników danych			X	
MA12	Kradzież laptopów poza siedzibą i pomieszczeniami instytucji			X	
MA17	Kradzież sprzętu i urządzeń informatycznych i telekomunikacyjnych wewnątrz pomieszczeń organizacji			X	
Błędy					
ER02	Przypadkowe skasowanie oprogramowania lub bibliotek			X	
ER05	Błąd w kodzie programu systemowego, oprogramowania, itp.				X
ER06	Błąd w programie aplikacyjnym				X

Etap III - Scenariusze zagrożeń

Skojarzenie zasobów z podatnościami

Scenariusz			Zasoby	Podatność
	Przyczyna			
		Pochodzenia : rodzaj ataku i/lub czynność		
01	Przejęciowa niedostępność zasobów			
01.10	Nieobecność personelu			
	01.12	Odejście z pracy personelu specjalistycznego (dobrowolne, zwolnienie itp.)	Personel specjalistyczny (administratorzy, projektanci itp.)	Odejście lub rezygnacja personelu strategicznego
01.20	Wypadek lub awaria jednego lub kilku zasobów sprzętowych			
	01.21a	Zwarcie instalacji elektrycznej powodujące uszkodzenie wyposażenia sieci (WAN, LAN, WIFI)		
02	Zniszczenie sprzętu			
02.20	Pożar			
	02.22c	Pożar w wyniku zwarcia instalacji elektrycznej, powodujący znaczne zniszczenie centralnych systemów informatycznych		
08	Ujawnienie danych lub informacji			
08.10	Dostęp do systemu i konsultacja			
	08.11a	Dostęp w trybie bezpośrednim do informacji służbowych przez hakera używającego portu otwartego na potrzeby sieci wewnętrznej	Informacje, dane lub wiadomości wymieniane, wysyłane itp.	Dostęp do danych współdzielonych i samowolne ich ujawnienie
	08.11b	Dostęp w trybie bezpośrednim do informacji służbowych przez osobę upoważnioną na terenie organizacji i podłączającą się do sieci wewnętrznej (poprzez np. wtyczkę sieciową w pomieszczeniu ogólnodostępna)		
	08.12	Dostęp do systemu w trybie bezpośrednim przez członka personelu posiadającego nielegalną autoryzację		

Etap IV – Ocena i oszacowanie ryzyka

Proces analizy scenariusza zagrożenia



Waga scenariusza zagrożenia jest funkcją jego prawdopodobieństwa oraz skutku. Otrzymaną macierz nazywamy macierzą akceptacji ryzyka, która definiuje akceptowalność ryzyka w funkcji jego szacowanego prawdopodobieństwa oraz skutku.

Skutek	Ryzyko			
I=4	S=2	S=3	S=4	S=4
I=3	S=2	S=3	S=3	S=4
I=2	S=1	S=2	S=2	S=3
I=1	S=1	S=1	S=1	S=2
	P=1	P=2	P=3	P=4

Prawdop.

- Na macierzy akceptacji ryzyka wyróżnia się 3 kategorie ryzyk:

Skutek	Ryzyko			
I=4	S=2	S=3	S=4	S=4
I=3	S=2	S=3	S=3	S=4
I=2	S=1	S=2	S=2	S=3
I=1	S=1	S=1	S=1	S=2
	P=1	P=2	P=3	P=4

Prawdop.

- ✓ ryzyko krytyczne (wymagające natychmiastowych działań poza normalnym budżetem (czerwony kolor)),
- ✓ ryzyko nieakceptowalne (wymagające działań eliminujących je w ramach planowanego budżetu (żółty kolor)),
- ✓ ryzyko akceptowalne (zielony kolor).

Analiza ryzyka

Oprogramowanie do analizy ryzyka

„Risicare”

oparte na metodzie Mehari

<http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Overview-PL.pdf>


Etapy Analizy Ryzyka w/g. Mehari

Zrzut ekranu Risicare

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

Risicare 2007



Risicare po łacinie oznacza "ryzykować"

Workflow Wykres audytu | Audyt | Wartości | Wykresy | Tematy | ISO 27002 | Kartografia | Podatność | Scenariusz | Działanie szczególne | Działanie ogólne | Ocena ryzyka

Wykres audytu: Standard

Audyt: Do zakończenia

- Wartości
- Wykresy
- Tematy
- ISO 27002

Kartografia: Niezakończona

Podatność: Standard

Scenariusz: Zrobione

Ocena ryzyka

Działanie szczególne: Zrobione

Działanie ogólne: Do wykonania

Wykres audytu : Faza z zebranymi danymi, bez wyników

Wykres audytu

Moja sytuacja : Standard

Wykres audytu	Zrobione
Własności komórek	Niezakończona
Zabronione kombinacje	Do zakończenia

Komentarze Risicare :
Co najmniej dwie domeny mają więcej niż jedną komórkę i nie wybrano zabronionych kombinacji
Te zabronione kombinacje umożliwiają zmniejszenie liczby replikacji scenariusza

Audyt zakończ 127 pytanie(a) - 0 bez odpowiedzi , 21 Bez przedmiotowo, 72 Tak, 34 Nie

PL 08:43 2010-09-02

Etapy Analizy Ryzyka w/g. Mehari

Wyniki audytu dla wszystkich domen bezpieczeństwa

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

Plan działania : Zakończ

Obszar roboczy

Wykres audytu

Komórka : D1 Nowe Pomoc Anuluj OK

Workflow Wykres audytu Audyt **Wartosci** Wykresy Tematy ISO 27002 Kartografia Podatnosc Scenariusz Dzialanie szczegolne Dzialanie ogolne Ocena

Początkowa całkowita ilość punktów : 1.93 - końcowa : 2.64 Całkowita ilość punktów jest średnia arytmetyczna wartości.

Pole	Komórka	Nazwa	Wartość P	Wartość K
A		Organizacja Bezpieczeństwa	2.02	2.28
A1	A1	A1 Nowe	2.02	2.28
B		Bezpieczeństwo siedziby (siedziba wraz z budynkiem)	2.69	3.77
B1	B1	B1 Nowe	2.69	3.77
C		Bezpieczeństwo pomieszczeń (pomieszczenia wraz z korytarzami itp.)	2.19	2.26
C1	C1	C1 Nowe	2.10	2.17

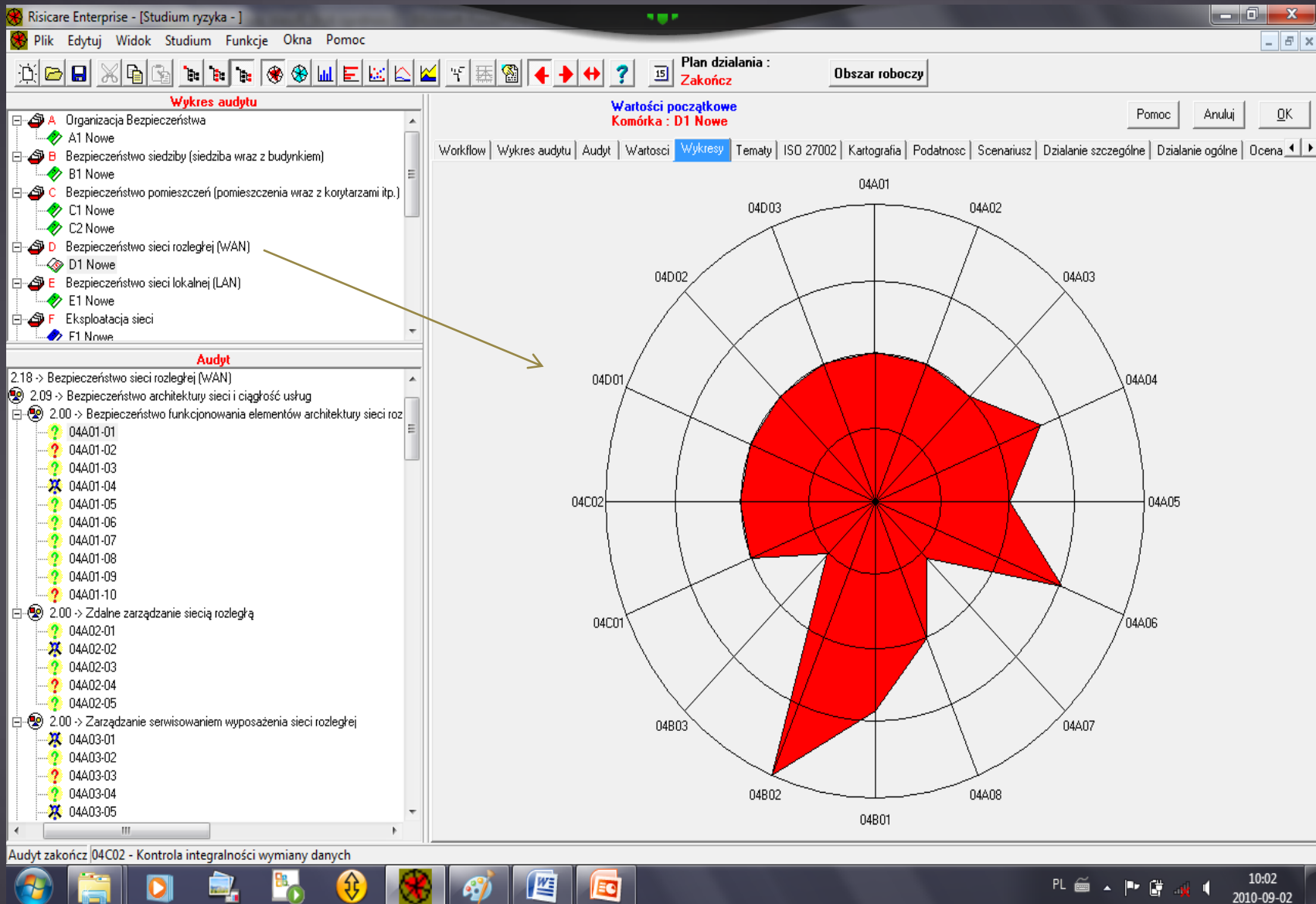
Wartości początkowe dla komórek

Audyt zakończ 127 pytanie(a) - 0 bez odpowiedzi , 21 Bez przedmiotowo, 72 Tak, 34 Nie

10:00 2010-09-02

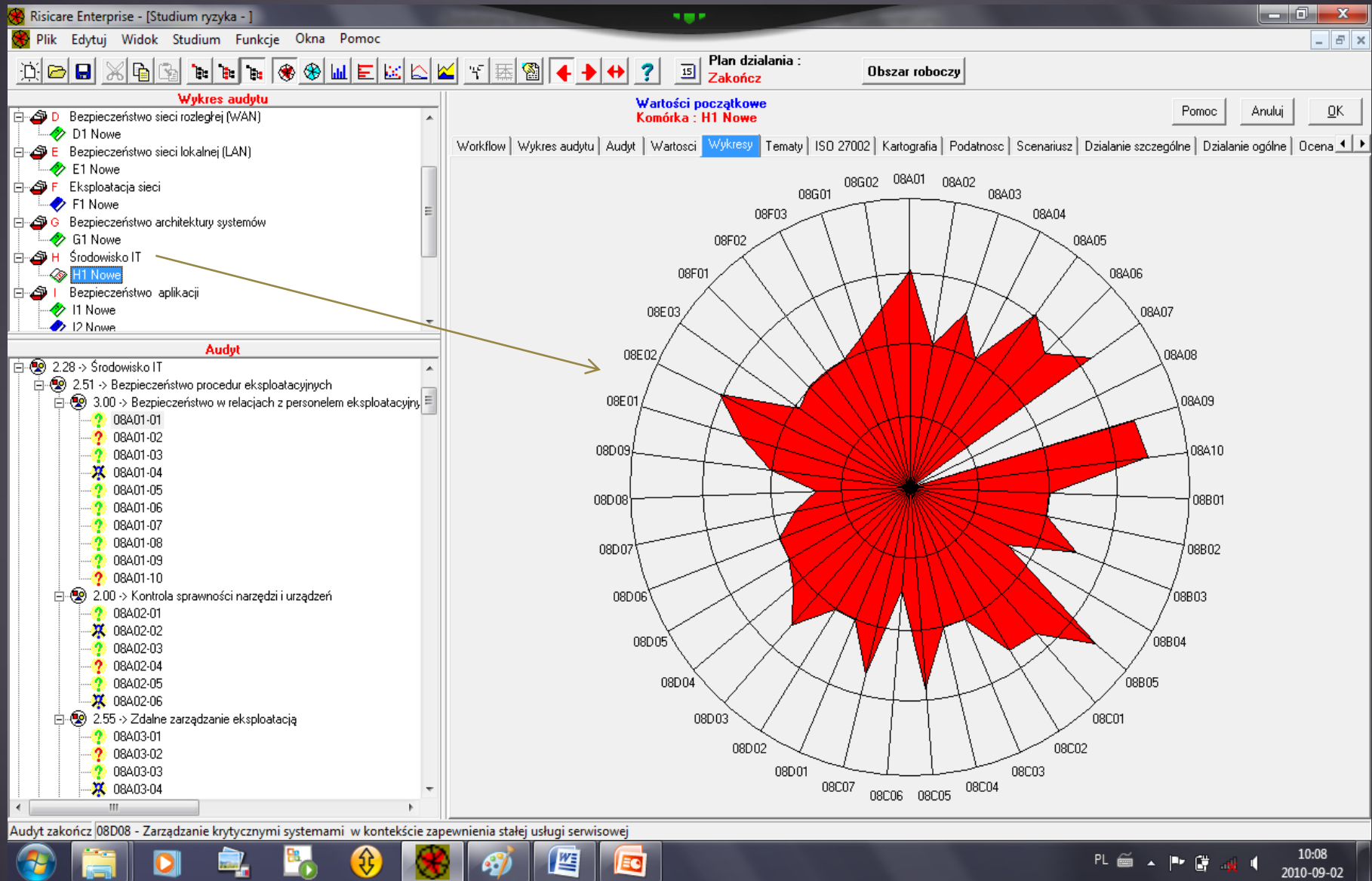
Etapy Analizy Ryzyka w/g. Mehari

Wynik audytu dla domeny bezpieczeństwa WLAN



Etapy Analizy Ryzyka w/g. Mehari

Wynik audytu dla domena bezpieczeństwa środowiska IT



Etapy Analizy Ryzyka w/g. Mehari

Wynik audytu dla ważniejszych domen bezpieczeństwa

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

zasady obliczania: Plan działania : Zakończ Obszar roboczy

Tematy

- 1.95 -> Zarządzanie bezpieczeństwem
 - 2.11 -> Rola i struktura organizacji
 - 1.78 -> Uświadamianie i szkolenia z bezpieczeństwa
- 2.32 -> Bezpieczeństwo fizyczne
 - 2.69 -> Kontrola dostępu do budynku
 - 2.19 -> Kontrola dostępu do pomieszczeń
 - 2.07 -> Różne ryzyka
- 1.50 -> Sieci i telekomunikacja
 - 1.19 -> Architektura sieciowa i systemowa
 - 1.81 -> Kontrola wymiany danych
- 1.61 -> Architektura systemów i aplikacji
 - 1.92 -> Kontrola dostępu logicznego
 - 1.29 -> Bezpieczeństwo danych
- 2.18 -> Eksploatacja systemów i sieci
 - 2.04 -> Procedury eksploatacyjne
 - 2.32 -> Zarządzanie nośnikami
- 1.62 -> Bezpieczeństwo funkcjonowania sieci
 - 1.11 -> Plany awaryjne
 - 2.32 -> Kopie zapasowe
 - 1.43 -> Serwis
- 1.83 -> Bezpieczeństwo podczas rozwoju aplikacji
 - 1.83 -> Projekt i wytwarzanie
- 2.13 -> Wykrywanie i zarządzanie incydentami
 - 2.13 -> Zarządzanie awariami

Pomoc Anuluj OK

Workflow Wykres audytu Audyt Wartości Wykresy **Tematy** ISO 27002 Kartografia Podatność Scenariusz Działanie szczególne Działanie ogólne Ocena

Początkowa całkowita ilość punktów: 1.89 - końcowa: 2.58 Tematy : Poziomy 1

Kod	Nazwa	Wartość P	Wartość K
A	Zarządzanie bezpieczeństwem	1.95	2.48
B	Bezpieczeństwo fizyczne	2.32	2.99
C	Sieci i telekomunikacja	1.50	2.88
D	Architektura systemów i aplikacji	1.61	2.31
E	Eksploatacja systemów i sieci	2.18	2.60
F	Bezpieczeństwo funkcjonowania sieci	1.62	2.00
G	Bezpieczeństwo podczas rozwoju aplikacji	1.83	2.50

Diagram rozetkowy : Tematy / Poziomy 1

10:14
2010-09-02

Etapy Analizy Ryzyka w/g. Mehari

Zgodność z ISO/IEC 27001

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

zasady obliczania: **Plan działania: Zakończ** Obszar roboczy

ISO 27002

Workflow Wykres audytu Audyt Wartości Wykresy Tematy **ISO 27002** Kartografia Podatność Scenariusz Działanie szczególne Działanie ogólne Ocena

Początkowa całkowita ilość punktów: 2.08 - końcowa: 2.34 ISO 27002 : Poziomy 1

Kod	Nazwa	Wartość P	Wartość K
5	Polityka bezpieczeństwa	2.00	2.00
6	Organizacja bezpieczeństwa informacji	2.10	2.23
7	Zarządzanie aktywami	2.00	2.00
8	Bezpieczeństwo zasobów ludzkich	1.85	1.85
9	Bezpieczeństwo fizyczne i środowiskowe	2.92	3.36
10	Zarządzanie systemami i sieciami	2.14	2.58
11	Kontrola dostępu	2.38	2.50

Diagram rozetkowy : ISO 27002 / Poziomy 1

10:19
2010-09-02

Etapy Analizy Ryzyka w/g. Mehari

Klasyfikacja zasobów

The screenshot displays the Riscare Enterprise software interface for risk analysis. The window title is "Riscare Enterprise - [Studium ryzyka -]". The menu bar includes "Plik", "Edytuj", "Widok", "Studium", "Funkcje", "Okna", and "Pomoc". The toolbar contains various icons for file operations and analysis. The main interface is divided into three panes:

- Left Pane (Kartografia):** A tree view showing a hierarchy of assets and controls. The selected item is "A01 - Doprogramowanie, middleware (kody wykonywalne)". Other items include "D01 - Pliki danych lub bazy danych", "R01 - Okablowanie, sprzęt i oprogramowanie sieciowe WAN", "S01 - Główne systemy i serwery hostingowe", "E01 - Miejsce i otoczenie pracy", "P01 - Personel specjalistyczny", and "C01 - Niezgodność z prawem i regulacjami dotyczącymi ochrony prywatności".
- Center Pane (Cel tej kartografii):** A form for defining the purpose of the mapping. It includes a table for "podstawowe kryteria" (basic criteria) and "Skutek istotny" (significant impact).

podstawowe kryteria	Skutek istotny
Dostępność	4
Integralność	
Poufność	
- Right Pane (Scenariusz dla kryterium dla kryterium : Dostępność):** A list of scenarios for the selected criterion. The scenarios include:
 - Przejęciowa niedostępność zasobów
 - Błąd oprogramowania
 - (1/1) - Niedostępność krytycznej aplikacji w wyniku błędu oprogramowania
 - (1/1) - Niedostępność krytycznej aplikacji w wyniku błędu oprogramowania
 - Niedostępność serwisu
 - (0/2) - Blokada aplikacji niemożliwa do usunięcia przez obsługę z powodu
 - Obniżenie wydajności
 - Modyfikacja oprogramowania
 - (0/1) - Niezamierzone obniżenie wydajności aplikacji podczas czynności s
 - Przypadkowe przeciążenie zasobów informatycznych lub sieciowych
 - (0/1) - Obniżenie wydajności aplikacji wynikające z przypadkowego nasyc
 - Celowe przeciążenie zasobów informatycznych lub sieciowych
 - (0/1) - Obniżenie wydajności aplikacji wynikające z celowego i powtarzając
 - Zniszczenie oprogramowania
 - Usuwanie kodu wykonywalnego lub danych konfiguracyjnych
 - (0/1) - Usuwanie kodu wykonywalnego przez osobę uprawnioną (persone
 - Przypadkowe zniszczenie napędu dysku stałego
 - (0/1) - Przypadkowe zniszczenie napędu dysku stałego i usuwanie progr
 - Przypadkowe usuwanie oprogramowania
 - (0/1) - Przypadkowe usuwanie oprogramowania wykonywalnego w wynik

Etapy Analizy Ryzyka w/g. Mehari

Klasyfikacja podatności zasobów

The screenshot displays the Risicare Enterprise application window. The left sidebar lists various assets under 'Podatność naturalna' (Natural Vulnerability) and 'Działania Celowe' (Deliberate Actions). The main area shows the 'Audyt : Faza z zebranymi danymi, bez wyników' (Audit: Phase with collected data, no results) for asset MA09. A pink bar indicates a 'Podatność : 3 Prawdopodobne' (Vulnerability: 3 Probable). Below this, a section titled 'Jaki jest poziom podatności' (What is the level of vulnerability) shows radio buttons for 'Bardzo nieprawdopodobne', 'Nieprawdopodobne', 'Prawdopodobne' (selected), and 'Bardzo prawdopodobne'. To the right, a vertical bar shows 'Podatność = 3'. The rightmost pane displays a 'Scenariusz z tym zdarzeniem' (Scenario with this event) with a tree view of potential impacts, such as 'Ujawnienie danych lub informacji' (Data or information disclosure) and 'Kradzież dokumentów' (Document theft).

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

Obszar roboczy

Podatność naturalna

- AC14 - Blokada aplikacji lub systemu niemożliwa do usunięcia przez serwis z
- AC15 - Przypadkowe przeładowanie (nasylenie) zasobów
- AC16 - Wypadek podczas eksploatacji doprowadzający do zmiany danych
- AC17 - Wymazywanie danych lub konfiguracji spowodowane wirusem
- AC18 - Przypadkowa utrata plików danych w wyniku uruchomienia automatu
- AC19 - Przypadkowa utrata plików danych w wyniku starzenia lub zanieczyszczenia
- AC20 - Przypadkowa utrata plików danych w wyniku zniszczenia (crash) dysku

Działania Celowe

- MA01 - Wandalizm zewnętrzny: wrzucenie kamienia i innych przedmiotów z ulicy
- MA02 - Wandalizm wewnętrzny: uszkodzenie okablowania sieci, drobnego sprzętu
- MA03 - Sabotaż lub atak terrorystyczny z zewnątrz: materiały wybuchowe w siedzibie
- MA04 - Celowe przeładowania (powtarzające się nasylenia) urządzeń sieci
- MA05 - Przeładowania (nasylenia) sieci przez robaki
- MA06 - Samowolne skasowanie (bezpośrednie lub pośrednie) oprogramowania
- MA07 - Celowe zmiany (bezpośrednie lub pośrednie) funkcjonalności oprogramowania
- MA08 - Manipulacja danych lub podanie fałszywych danych na wejściu
- MA09 - Dostęp do danych współdzielonych i samowolne ich ujawnienie**
- MA10 - Przechwycenie plików i/lub kradzież nośników danych
- MA11 - Samowolne skasowanie (bezpośrednie lub pośrednie), kradzież lub uszkodzenie sprzętu
- MA12 - Kradzież laptopów poza siedzibą i pomieszczeniami instytucji
- MA13 - Celowe skasowanie konfiguracji sieci
- MA14 - Celowe skasowanie parametrów konfiguracyjnych aplikacji lub systemów
- MA15 - Przejęcie (defraudacja) kodu źródłowego oprogramowania lub aplikacji
- MA16 - Szpiegostwo etatowe i wymagające dużych nakładów, specjalistyczne
- MA17 - Kradzież sprzętu i urządzeń informatycznych i telekomunikacyjnych w siedzibie

Dobrowolne i niezamierzone działania

- AV01 - Nieobecność lub strajk personelu eksploatacyjnego
- AV02 - Odejsięcia lub rezygnacja personelu strategicznego
- AV03 - Penetracja systemu informacyjnego trzeciej strony przez personel organizacji
- AV04 - Nielegalne używanie w organizacji licencji na oprogramowanie lub produkty

Błędy

- ER01 - Niezamierzone pogorszenie wydajności aplikacji podczas serwisowania
- ER02 - Przypadkowe skasowanie oprogramowania lub bibliotek w wyniku błędów
- ER03 - Przypadkowa zmiana danych podczas serwisu
- ER04 - Błąd podczas gromadzenia danych
- ER05 - Błąd w kodzie programu systemowego, oprogramowania itp.
- ER06 - Błąd w programie aplikacyjnym
- ER07 - Błąd podczas modyfikacji funkcjonalności arkusza kalkulacyjnego lub bazy danych

Workflow Wykres audytu Audyt Wartości Wykresy Tematy ISO 27002 Kartografia Podatność Scenariusz Działanie szczególne Działanie ogólne

Audyt : Faza z zebranymi danymi, bez wyników

MA09

Dostęp do danych współdzielonych i samowolne ich ujawnienie

Standardowa podatność naturalna (dane z bazy wiedzy)

Podatność : 3 Prawdopodobne

Jaki jest poziom podatności

Bardzo nieprawdopodobne

Nieprawdopodobne

Prawdopodobne

Bardzo prawdopodobne

Podatność = 3

Komentarze :

Scenariusz z tym zdarzeniem

- Ujawnienie danych lub informacji
 - Dostęp do systemu i konsultacja
 - (0/2)- Dostęp w trybie bezpośrednim do informacji służbowych przez
 - (0/2)- Dostęp w trybie bezpośrednim do informacji służbowych przez
 - (0/2)- Dostęp do systemu w trybie bezpośrednim przez członka personelu
 - Przechwycenie przesyłanej informacji
 - (0/4)- Przechwycenie przez członka personelu, mającego uprawnienia
 - (0/2)- Przechwycenie przez członka personelu, uprawnionego do
 - (2/2)- Przechwycenie przez administratora sieci, za pomocą zmod
 - (2/2)- Przechwycenie przez hakera, wykorzystującego zdalne łąc
 - (2/2)- Przechwycenie przez hakera, wykorzystującego znaną, lecz
 - (1/1)- Przechwycenie, poprzez podsłuch, wymienianych wiadomości
 - (2/2)- Przechwycenie wymienianych wiadomości w sieci organizac
 - (1/1)- Przekierowanie wrażliwych danych przechwycenych przez
 - Kradzież dokumentów napisanych odręcznie lub wydrukowanych
 - (1/1)- Kradzież wykazów (listings) lub wydruków podczas ich dyst
 - (2/2)- Kradzież wykazów (listings) lub wydruków przez pracownik
 - (0/1)- Powtarzająca się kradzież dokumentów przez członka personelu
 - (0/1)- Powtarzająca się kradzież dokumentów przez byłego członka
 - (0/1)- Kradzież dokumentów przez klienta z pomieszczeń organizac
 - (1/1)- Kradzież dokumentów przez szpiega, który nielegalnie dost
 - (0/1)- Kradzież przez osobę (z personelu sprzątającego, ochrony
 - (0/1)- Kradzież z kancelarii korespondencji wrażliwej poza godzin
 - Przekierowanie informacji podczas transmisji
 - (1/1)- Przekierowanie faksów kradzieży z pomieszczeń wypos
 - (0/1)- Nieuprawnione przekierowanie faksów przy wykorzystaniu
 - Przekierowanie informacji tymczasowej tworzonej przez system
 - (0/1)- Przekierowanie przez administratora informacji nieusuniętych

Etapy Analizy Ryzyka w/g. Mehari

Zobrazowane wyniki analizy ryzyka dla każdego ze scenariuszy zagrożeń

Risicare Enterprise - [Studium ryzyka -] Save time with computer shortcuts

Plik Edytuj Widok Studium Funkcje Okna Pomoc

Plan działania : Zakończ Obszar roboczy

Scenariusz (początkowe G)

Całkowita liczba kombinacji : 344 - z 48 wybranymi

Workflow Wykres audytu Audyt Wartości Wykresy Tematy ISO 27002 Kartografia Podatność Scenariusz Działanie szczególne Działanie ogólne Ocena ryzyka

Scenariusz : 01.31 a
Dostępność
Na obiekcie (Klasyf. zasobu : 4) : A01 - Oprogramowanie, middleware (kody wykonywalne)

Komórki uwzględnione przez ten scenariusz

Komórki audytu	Pr	Sk	POW
✓ A1H1	4	3	4

Szczegóły Status Personalizacja Opis

Wartości początkowe

Prawdopodobieństwo, Skutek, Waga

Podat: 4
Odradz: -
Zapob: 2

Ochrona: -
Łagodz: 2
Odzysk: 2

Prawdopodobieństwo: 4

Waga: 4

ESR: 2

Skutek: 3

klasyf. zasobu: 4

18:35
2010-09-02

Etapy Analizy Ryzyka w/g. Mehari

Waga ryzyka dla wszystkich scenariuszy

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

Plan działania : Zakończ Obszar roboczy

Scenariusz (Początkowa G)

Powaga początkowa

Workflow Wykres audytu Audyt Wartości Wykresy Tematy ISO 27002 Kartografia Podatność Scenariusz Działanie szczególne Działanie ogólne Ocena ryzyka

Powaga początkowa			
Grupa	Nazwa grupy scenariuszy	Powaga początkowa	Powaga końcowa
01	Przejęciowa niedostępność zasobów	4	3
03	Obniżenie wydajności	4	1
05	Zmiana oprogramowania	4	1
nc	Zmiana danych	4	1

Wykres babelkowy

Etapy Analizy Ryzyka w/g. Mehari

Waga ryzyka dla wszystkich scenariuszy

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

Plan działania :
Zakończ Obszar roboczy

Scenariusz [Początkowa G]

Powaga początkowa

Pomoc Anuluj OK

Workflow Wykres audytu Audyt Wartości Wykresy Tematy ISO 27002 Kartografia Podatność Scenariusz Działanie szczególne Działanie ogólne **Ocena ryzyka**

Liczba scenariuszy dla prawdopodobieństwa i skutku

Prawdopodobieństwo

Rodziny scenariuszy

Wykres bąbelkowy

Skutek

Prawdopodobieństwo	Skutek	Liczba scenariuszy
3	4	1
4	4	1
3	3	15

- Modyfikacja sprzętu
- Przypadkowe przeciężenie zasobów informatycznych lub si
- Celowe przeciężenie zasobów informatycznych lub sieciowj
- Zniszczenie oprogramowania
- Usuwanie kodu wykonywalnego lub danych konfiguracyjny
- Przypadkowe zniszczenie napędu dysku stałego
- Przypadkowe usuwanie oprogramowania
- Kradzież lub usuwanie zawartości przenośnego nośnika dai
- Usuwanie lub zniszczenie danych konfiguracyjnych progr
- Zmiana oprogramowania
- Zmiana danych
- Wypadek podczas przetwarzania danych
- Błąd gromadzenia danych
- Manipulacja danymi
- Ujawnienie danych lub informacji
- Dostęp do systemu i konsultacja
- Przechwycenie przesyłanej informacji
- Kradzież dokumentów napisanych odręcznie lub wydrukow
- Przekierowanie informacji podczas transmisji
- Przekierowanie informacji tymczasowej tworzonej przez syst
- Przekierowanie plików danych
- Dostęp do systemu i kopiowanie plików danych aplikacji biz
- Kradzież nośników danych aplikacji służbowych
- Dostęp do serwerów i kopii plików biurowych
- Przekierowanie kodu źródłowego oprogramowania
- Utrata plików danych lub dokumentów
- Usuwanie danych przez bombę logiczną
- Usuwanie zawartości nośników danych przez wirusy
- Celowe usuwanie zawartości nośników
- Przypadkowa utrata plików
- Kradzież nośników
- Przypadkowa utrata dokumentów
- Katastrofa wpływająca globalnie na dane
- Usuwanie plików przez bombę logiczną
- Zamierzone usuwanie zawartości nośników danych
- Niezgodność z wymaganiami prawa i obowiązującymi przepis
- Zdalny atak innej organizacji
- Naruszenie praw własności intelektualnej

10:58
2010-09-02

Etapy Analizy Ryzyka w/g. Mehari

Manualny interfejs wyboru środków zaradczych

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

Plan działania : Zakończ Obszar roboczy

Wykres audytu

Koszt bezpośredni (k€) : 2200 Koszt pośredni (JxH) 3000

Pomoc Anuluj OK

Workflow Wykres audytu Audyt Wartości Wykresy Tematy ISO 27002 Kartografia Podatność Scenariusz Działanie szczególne **Działanie ogólne** Ocena ryzyka

Ogólny plan działania dla komórki ...

Uwaga	Kod	Podusługa
2.2	08G...	Kontrola funkcjonowania audytu
2.7	08C07	Fizyczne bezpieczeństwo obrotu (wynoszenia) nośnikami
3.3	08A09	Zarządzanie procedurami związanymi z eksploatacją informatyczną
3.4	08A10	Zarządzanie dostawcami usług związanych z produkcją informatyczną

Ogólny plan działania

Kod	Podusługa	Komórka	Wartość początkowa	Wartość końcowa	Koszt bezpośredni	Koszt pośredni	Data początku	Data zakończenia
08G02	Ochrona narzędzi i wyników audytów	H1 Nowe	2.5	4.0	2000	0	9/2/2010	9/2/2010
08A01	Bezpieczeństwo w relacjach z personelem eksploatacyjnym (personel na umowę stałą i kontrahenci)	H1 Nowe	3.0	4.0	200	3000	9/2/2010	9/2/2010

Wykres audytu

- A Organiza
 - A1 Nowe
- B Bezpiecz
 - B1 Nowe
- C Bezpiecz
 - C1 Nowe
- D Bezpiecz
 - D1 Nowe
- E Bezpiecz
 - E1 Nowe
- F Eksploat.
 - F1 Nowe
- G Bezpiecz
 - G1 Nowe
- H Środowis
 - H1 Nowe
- I Bezpiecz
 - I1 Nowe
 - I2 Nowe
- J Bezpiecz
 - J1 Nowe
- K Bezpiecz
 - K1 Nowe
- L Bezpiecz
 - L1 Nowe

10:49
2010-09-02

Etapy Analizy Ryzyka w/g. Mehari

Zautomatyzowany interfejs wyboru środków zaradczych

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

Plan działania : Zakończ Obszar roboczy

Koszt bezpośredni (k€): 0 Koszt pośredni (JxH) 0

Workflow | Wykres audytu | Audyt | Wartości | Wykresy | Tematy | ISO 27002 | Kartografia | Podatność | Scenariusz | **Działanie szczególne** | Działanie ogólne | Ocena ryzyka

Scenariusz poprawiony przez wybrana usługa

Dane dla wybranego powyżej scenariusza

Scenariusz :
Status :
Frawdopodobieństwo
Expo :
DISS :
PREV :
Skutek
PRDT :
PALL :
RECUP :

Szczególny plan działania | Komentarze | Zapis

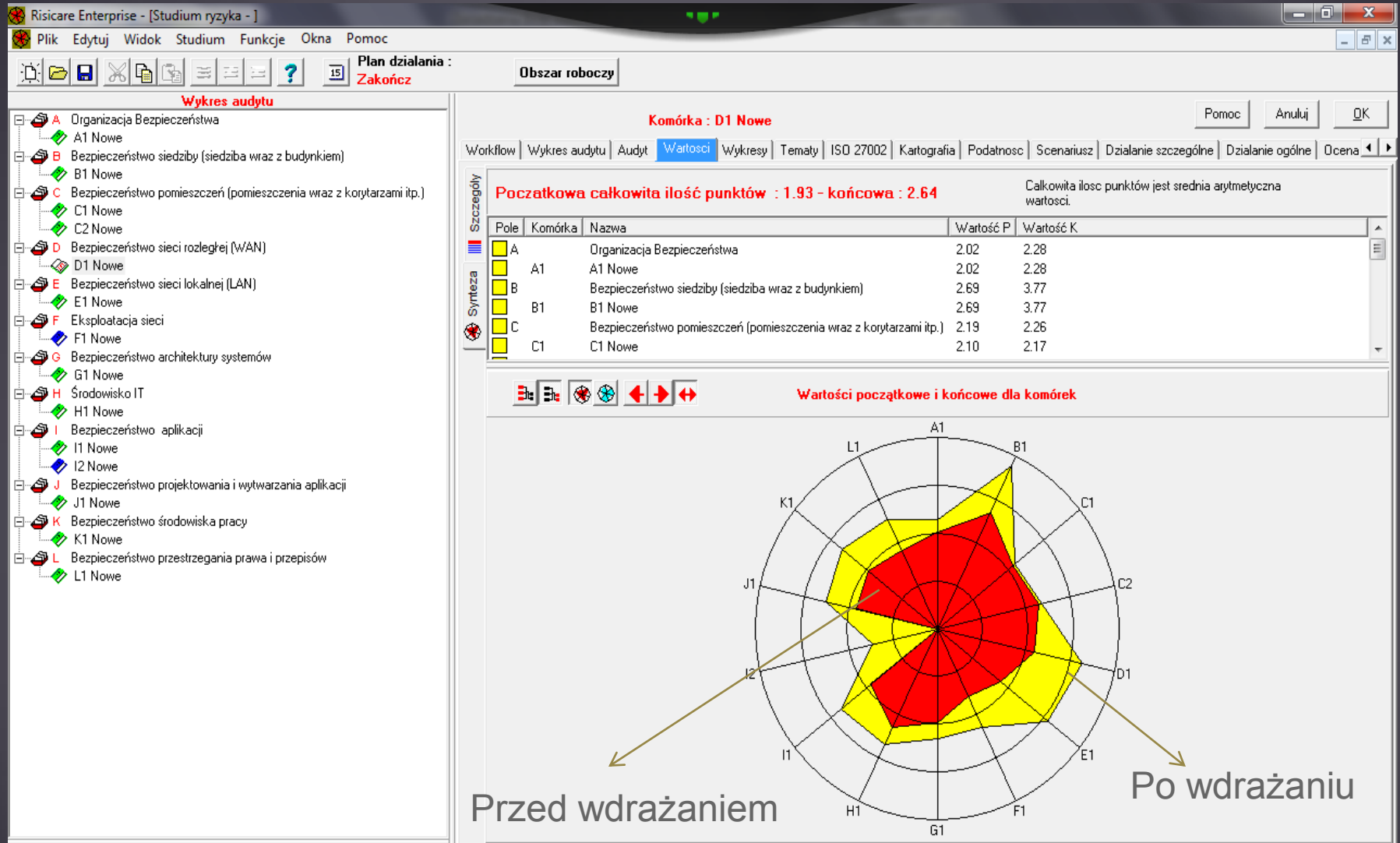
Szczegółowy plan działania

Kod	Podusługa	Komó...	Wartość początkowa	Wartość końcowa	Koszt bezpośredni	Koszt pośredni	Data początku	Data zakończenia
09C01	Szyfrowanie wymiany d...	I2 No...	0.0	4.0	0	0	7/11/2010	7/11/2010
09C01	Szyfrowanie wymiany d...	I1 No...	0.0	4.0	0	0	7/11/2010	7/11/2010
08B02	Kontrola zgodności kon...	H1 N...	2.0	4.0	0	0	7/11/2010	7/11/2010
05C04	Ochrona integralności ...	E1 N...	1.3	4.0	0	0	7/11/2010	7/11/2010
05B07	Filtrowanie dostępu do ...	E1 N...	0.7	4.0	0	0	7/11/2010	7/11/2010
02A03	Kontrola dostępu do sie...	B1 N...	1.0	4.0	0	0	7/11/2010	7/11/2010
05B05	Uwierzytelnienie użytko...	E1 N...	2.0	4.0	0	0	7/11/2010	7/11/2010
04B03	Uwierzytelnianie podmio...	D1 N...	1.0	4.0	0	0	7/11/2010	7/11/2010
12A02	Przestrzeganie prawa d...	L1 No...	1.6	4.0	0	0	7/11/2010	7/11/2010
01D02	Ubezpieczenie od szkó...	A1 N...	1.6	4.0	0	0	7/11/2010	7/11/2010
12B01	Przestrzeganie prawa d...	L1 No...	1.5	4.0	0	0	7/11/2010	7/11/2010
05D02	Off-line'owe analizy ślad...	E1 N...	3.0	4.0	0	0	7/11/2010	7/11/2010
05A02	Bezpieczeństwo funkcj...	E1 N...	0.0	4.0	0	0	7/11/2010	7/11/2010
08A08	Dystrybucja wrażliwych ...	H1 N...	0.0	4.0	0	0	7/11/2010	7/11/2010
09C03	Ochrona przed promieni...	I1 No...	0.0	4.0	0	0	7/11/2010	7/11/2010
09C03	Ochrona przed promieni...	I2 No...	0.0	4.0	0	0	7/11/2010	7/11/2010
11B05	Bezpieczeństwo inform...	K1 N...	1.3	4.0	0	0	7/11/2010	7/11/2010
05C03	Szyfrowanie wymiany d...	E1 N...	2.0	4.0	0	0	7/11/2010	7/11/2010
05D02	Zapobieganie incydenta...	E1 N...	2.0	4.0	0	0	7/11/2010	7/11/2010



Etapy Analizy Ryzyka w/g. Mehari

Wyniki audytu dla domen bezpieczeństwa po wdrożeniu środków zaradczych

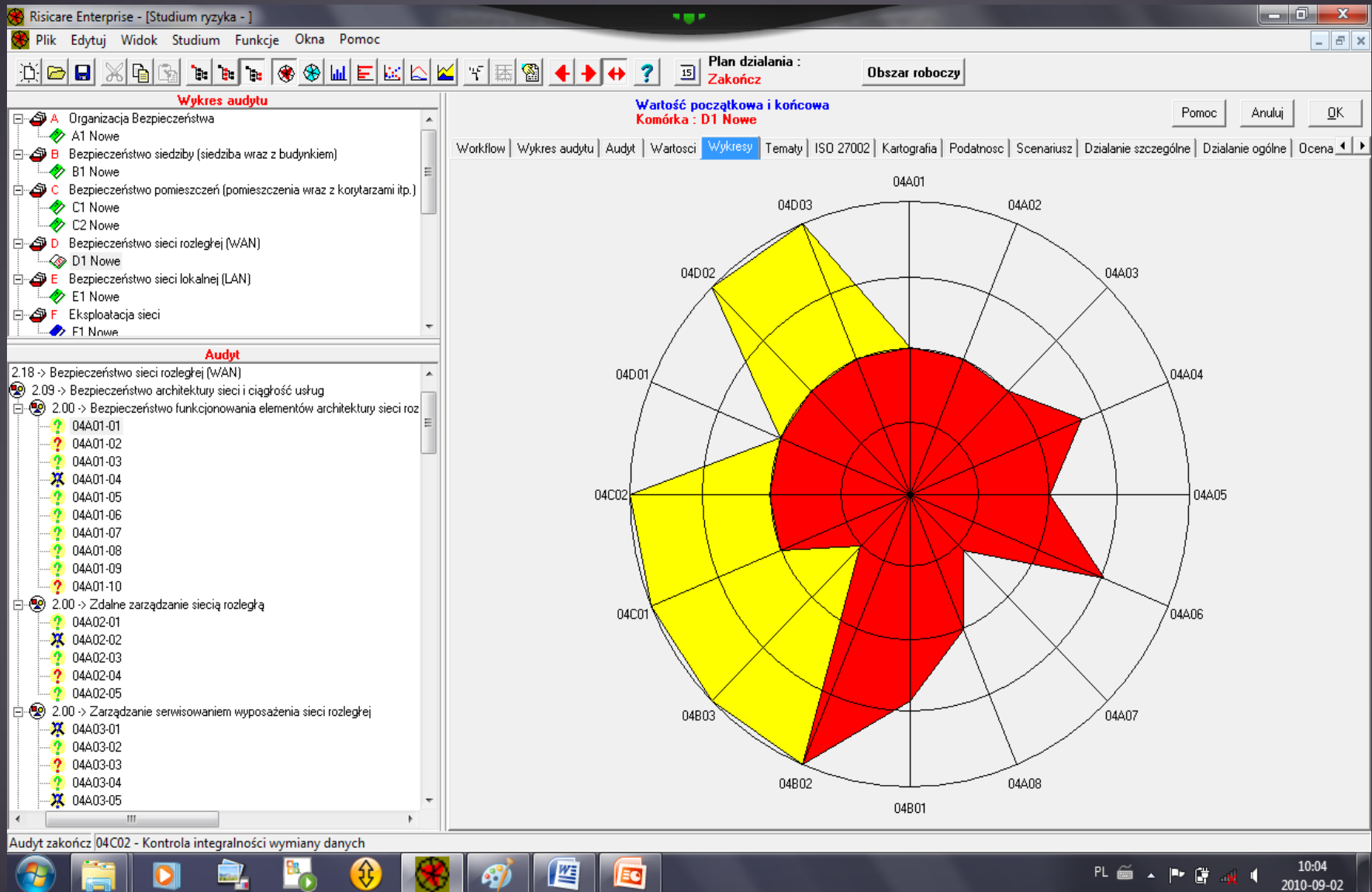


Audyt zakończ 127 pytanie(a) - 0 bez odpowiedzi, 21 Bez przedmiotowo, 72 Tak, 34 Nie



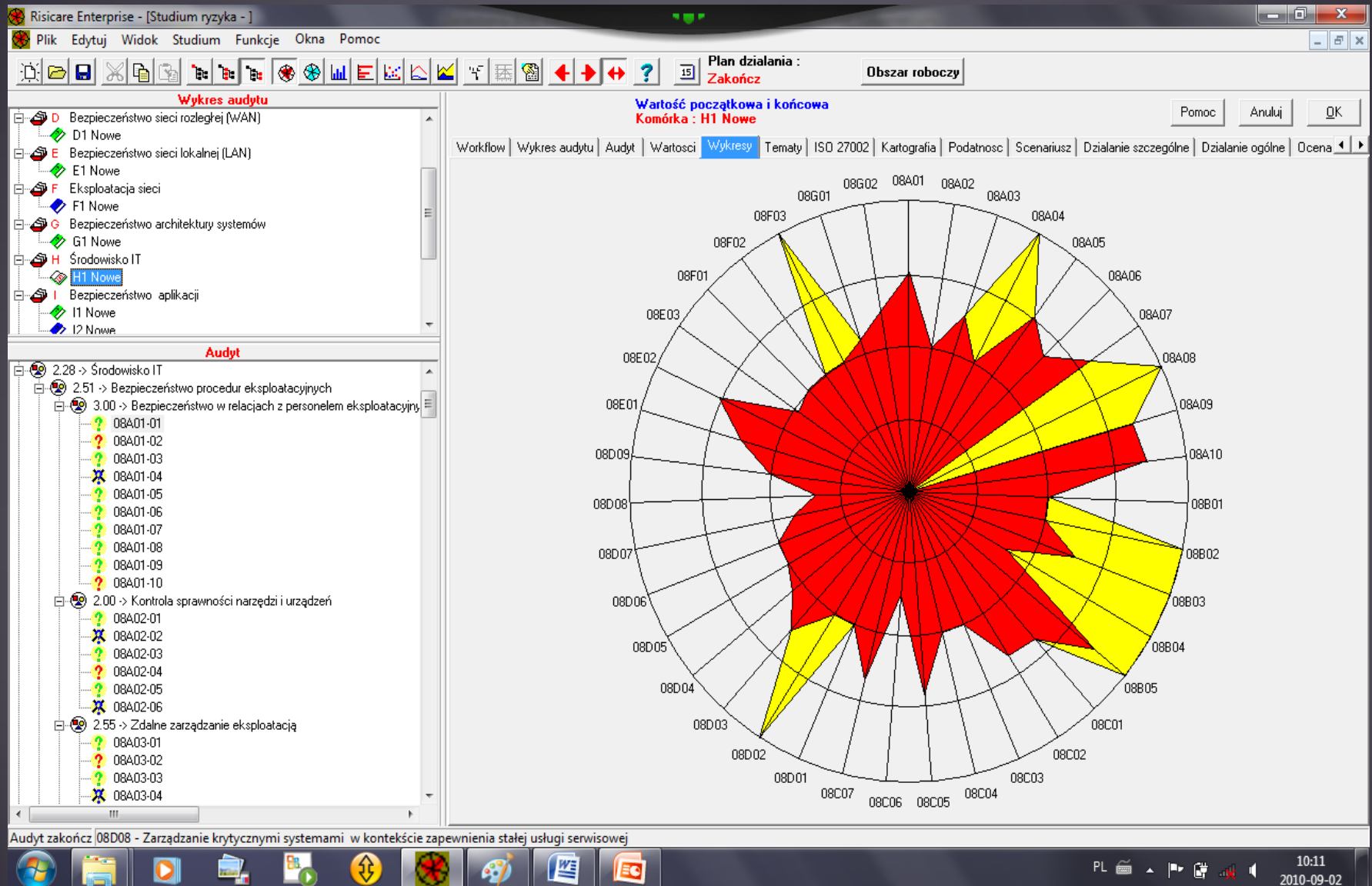
Etapy Analizy Ryzyka w/g. Mehari

Wyniki audytu dla WLAN'u po wdrożeniu środków zaradczych



Etapy Analizy Ryzyka w/g. Mehari

Wyniki audytu dla środowiska IT po wdrożeniu środków zaradczych



Etapy Analizy Ryzyka w/g. Mehari

Wynik audytu dla ważniejszych domen po wdrożeniu środków zaradczych

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

zasady obliczania : **Plan działania : Zakończ** Obszar roboczy

Pomoc Anuluj OK

Workflow Wykres audytu Audyt Wartości Wykresy **Tematy** ISO 27002 Kartografia Podatność Scenariusz Działanie szczególne Działanie ogólne Ocena

Początkowa całkowita ilość punktów: 1.89 - końcowa: 2.58 **Tematy : Poziomy 1**

Kod	Nazwa	Wartość P	Wartość K
A	Zarządzanie bezpieczeństwem	1.95	2.48
B	Bezpieczeństwo fizyczne	2.32	2.99
C	Sieci i telekomunikacja	1.50	2.88
D	Architektura systemów i aplikacji	1.61	2.31
E	Eksploatacja systemów i sieci	2.18	2.60
F	Bezpieczeństwo funkcjonowania sieci	1.62	2.00
G	Bezpieczeństwo podczas rozwoju aplikacji	1.83	2.50

Diagram rozetkowy : Tematy / Poziomy 1

Axis	Initial Score (P)	Final Score (K)
A	1.95	2.48
B	2.32	2.99
C	1.50	2.88
D	1.61	2.31
E	2.18	2.60
F	1.62	2.00
G	1.83	2.50

10:17
2010-09-02

Etapy Analizy Ryzyka w/g. Mehari

Zgodność systemu informacyjnego z ISO/IEC 27001 po wdrożeniu środków zaradczych

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

zasady obliczania : **Plan działania : Zakończ** Obszar roboczy

ISO 27002

- 2.00 -> Polityka bezpieczeństwa
- 2.00 -> Polityka bezpieczeństwa informacji
 - 0.00 -> Dokument polityki bezpieczeństwa informacji
 - 4.00 -> Przegląd polityki bezpieczeństwa informacji
- 2.10 -> Organizacja bezpieczeństwa informacji
- 2.21 -> Organizacja wewnętrzna
 - 4.00 -> Zaangażowanie kierownictwa w bezpieczeństwo informacyjne
 - 2.67 -> Koordynacja bezpieczeństwa informacji
 - 4.00 -> Przypisanie odpowiedzialności w zakresie bezpieczeństwa informacji
 - 0.00 -> Proces autoryzacji środków przetwarzania informacji
 - 3.00 -> Umowy o zachowaniu poufności
 - 0.00 -> Kontakty z organami władzy
 - 0.00 -> Kontakty z grupami zainteresowanymi bezpieczeństwem
 - 4.00 -> Niezależny przegląd bezpieczeństwa informacji
- 2.00 -> Strony zewnętrzne
 - 4.00 -> Określanie ryzyk związanych ze stronami zewnętrznymi
 - 0.00 -> Bezpieczeństwo w kontaktach z klientami
 - 2.00 -> Bezpieczeństwo w umowach ze stroną trzecią
- 2.00 -> Zarządzanie aktywami
 - 2.00 -> Odpowiedzialność za aktywa
 - 2.00 -> Inwentaryzacja aktywów
 - 4.00 -> Właśność aktywów
 - 0.00 -> Akceptowalne użycie aktywów
 - 2.00 -> Klasyfikacja informacji
 - 2.00 -> Zalecenia do klasyfikacji
 - 2.00 -> Oznaczanie i postępowanie z informacjami
- 1.85 -> Bezpieczeństwo zasobów ludzkich
 - 1.11 -> Przed zatrudnieniem
 - 0.00 -> Role i odpowiedzialności
 - 1.33 -> Postępowanie sprawdzające
 - 2.00 -> Zasady i warunki zatrudnienia
 - 0.44 -> Podczas zatrudnienia
 - 0.00 -> Odpowiedzialność kierownictwa
 - 1.33 -> Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa
 - 0.00 -> Postępowanie dyscyplinarne
 - 4.00 -> Zakończenie lub zmiana zatrudnienia
 - BP -> Odpowiedzialność związana z zakończeniem zatrudnienia
 - 4.00 -> Zwrot aktywów
 - 4.00 -> Przebranie praw dostępu

Workflow Wykres audytu Audyt Wartości Wykresy Tematy **ISO 27002** Kartografia Podatność Scenariusz Działanie szczególne Działanie ogólne Ocena

Początkowa całkowita ilość punktów: 2.08 - końcowa: 2.34 ISO 27002 : Poziomy 1

Kod	Nazwa	Wartość P	Wartość K
5	Polityka bezpieczeństwa	2.00	2.00
6	Organizacja bezpieczeństwa informacji	2.10	2.23
7	Zarządzanie aktywami	2.00	2.00
8	Bezpieczeństwo zasobów ludzkich	1.85	1.85
9	Bezpieczeństwo fizyczne i środowiskowe	2.92	3.36
10	Zarządzanie systemami i sieciami	2.14	2.58
11	Kontrola dostępu	2.38	2.50

Diagram rozetkowy : ISO 27002 / Poziomy 1

10:21
2010-09-02

Etapy Analizy Ryzyka w/g. Mehari

Zobrazowanie ryzyka dla każdego ze scenariuszy po wdrożeniu środków zaradczych

Risicare Enterprise - [Studium ryzyka -]

Bus hits roadside bomb, killing 25 in Afghanistan

Plik Edytuj Widok Studium Funkcje Okna Pomoc

Plan działania : Zakończ

Obszar roboczy

Scenariusz (początkowe G)

Całkowita liczba kombinacji : 344 - z 48 wybranymi

Workflow Wykres audytu Audyt Wartości Wykresy Tematy ISO 27002 Kartografia Podatność Scenariusz Działanie szczególne Działanie ogólne Ocena ryzyka

Scenariusz : 01.31a
Dostępność
Na obiekcie (Klasyf. zasobu : 4) : A01 - Oprogramowanie, middleware (kody wykonywalne)

Komórki uwzględnione przez ten scenariusz

- A - Organizacja Bezpieczeństwa
 - A1 Nowe
- H - Środowisko IT
 - H1 Nowe

Komórki audytu	Pr	Sk	POW
✓ A1H1	4	3	4

Szczegóły Status Personalizacja Opis

Wartości końcowe

Prawdopodobieństwo, Skutek, Waga

Podat: 4
Odradz: -
Zapob: 4

Prawdopodobieństwo: 1

Ochrona: -
Łagodź: 4
Odzysk: 4

ESR: 3

Skutek: 2

Waga: 1

klasyf. zasobu: 4

18:37
2010-09-02

Etapy Analizy Ryzyka w/g. Mehari

Ryzyko systemu po wdrożeniu środków zaradczych

Risicare Enterprise - [Studium ryzyka -]

Plik Edytuj Widok Studium Funkcje Okna Pomoc

Plan działania : Zakończ Obszar roboczy

Scenariusz (Początkowa P)

- Modyfikacja sprzętu
- Przypadkowe przeciężenie zasobów informatycznych lub sieci
- Celowe przeciężenie zasobów informatycznych lub sieci
- Zniszczenie oprogramowania
 - Usuwanie kodu wykonywalnego lub danych konfiguracyjnych
 - Przypadkowe zniszczenie napędu dysku stałego
 - Przypadkowe usuwanie oprogramowania
 - Kradzież lub usuwanie zawartości przenośnego nośnika danych
 - Usuwanie lub zniszczenie danych konfiguracyjnych oprogramowania
- Zmiana oprogramowania
- Zmiana danych
 - Wypadek podczas przetwarzania danych
 - Błąd gromadzenia danych
 - Manipulacja danymi
 - Ujawnianie danych lub informacji
 - Dostęp do systemu i konsultacja
 - Przechwycenie przesyłanej informacji
 - Kradzież dokumentów napisanych odręcznie lub wydruków
 - Przekierowanie informacji podczas transmisji
 - Przekierowanie informacji tymczasowej tworzonej przez system
- Przekierowanie plików danych
 - Dostęp do systemu i kopiowanie plików danych aplikacji biznesowych
 - Kradzież nośników danych aplikacji służbowych
 - Dostęp do serwerów i kopii plików biurowych
 - Przekierowanie kodu źródłowego oprogramowania
- Utrata plików danych lub dokumentów
 - Usuwanie danych przez bombę logiczną
 - Usuwanie zawartości nośników danych przez wirusy
 - Celowe usuwanie zawartości nośników
 - Przypadkowa utrata plików
 - Kradzież nośników
 - Przypadkowa utrata dokumentów
- Katastrofa wpływająca globalnie na dane
 - Usuwanie plików przez bombę logiczną
 - Zamierzone usuwanie zawartości nośników danych
- Niezgodność z wymaganiami prawa i obowiązującymi przepisami
 - Zdalny atak innej organizacji
 - Naruszenie praw własności intelektualnej

Powaga początkowa i końcowa

Workflow Wykres audytu Audyt Wartości Wykresy Tematy ISO 27002 Kartografia Podatność Scenariusz Działanie szczególne Działanie ogólne Ocena ryzyka

Powaga początkowa			
Grupa	Nazwa grupy scenariuszy	Powaga początkowa	Powaga końcowa
01	Przejściowa niedostępność zasobów	4	3
03	Obniżenie wydajności	4	1
05	Zmiana oprogramowania	4	1
nc	Zmiana danych	4	1

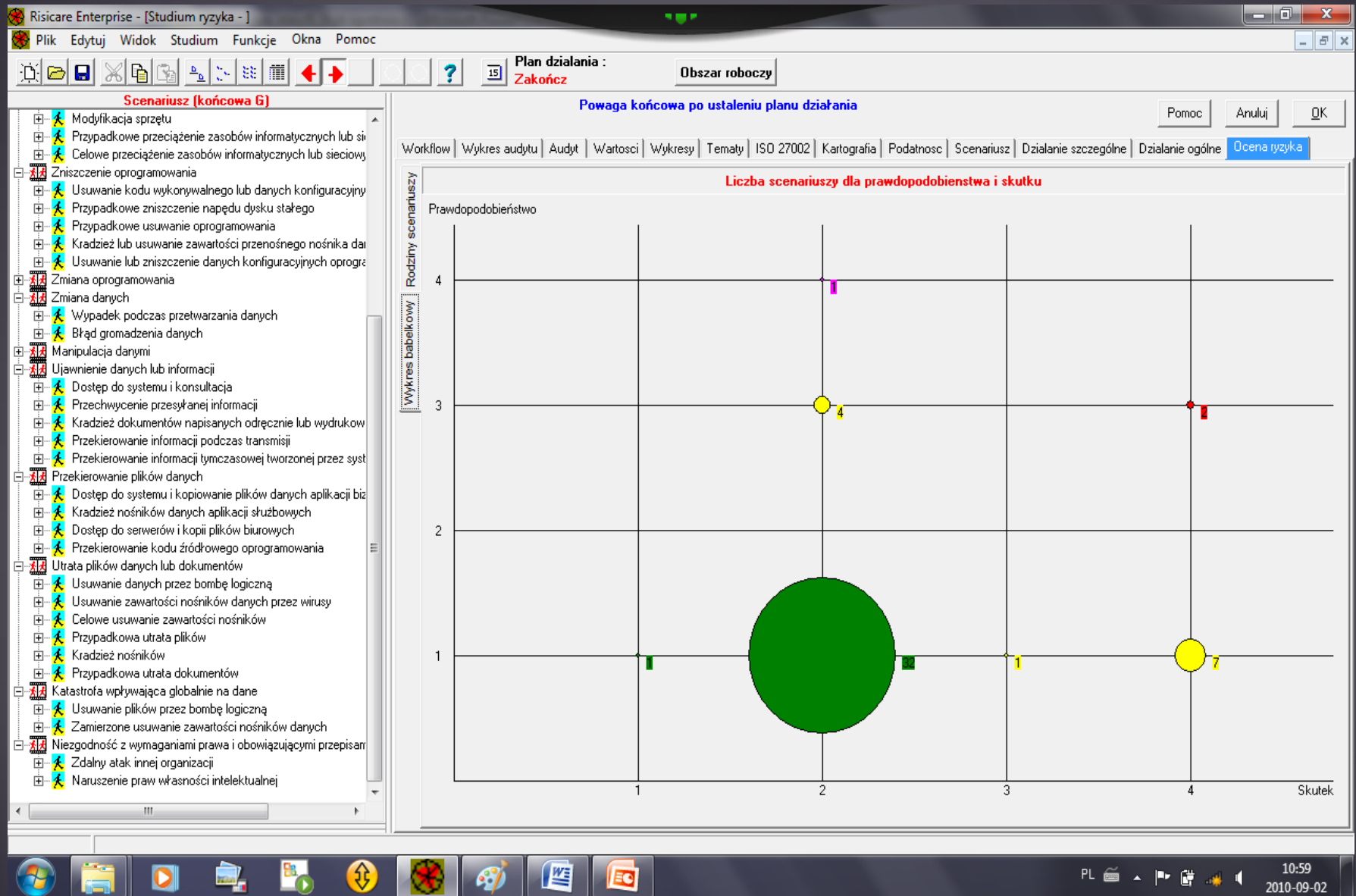
Powaga początkowa i końcowa

Wykres babelkowy

10:57
2010-09-02

Etapy Analizy Ryzyka w/g. Mehari

Ryzyko systemu po wdrożeniu środków zaradczych



BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH



AUDYTY i SZKOLENIA

”
Bezpieczeństwo - musi być nieodłączną częścią całościowego planu zarządzania organizacją, zintegrowanego ze wszystkimi procesami funkcjonalnymi zachodzącymi w organizacji.
”



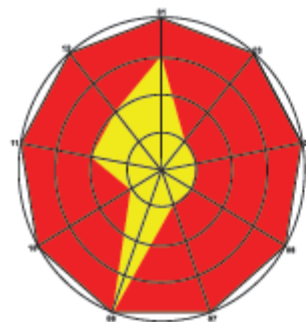
Audyt bezpieczeństwa teleinformatycznego obejmuje analizę i ocenę:

- ➔ zgodności systemów teleinformatycznych z obowiązującymi wymaganiami prawnymi,
- ➔ zgodności z wymaganiami normy ISO/IEC 27001 w zakresie Zarządzania Bezpieczeństwem Systemów Informatycznych (ZBSI),
- ➔ bezpieczeństwa konfiguracji i eksploatacji sieci (serwerów, routerów, przełączników itp.),
- ➔ bezpieczeństwa eksploatacji systemów operacyjnych i oprogramowania aplikacyjnego,
- ➔ skuteczności stosowanych rozwiązań w zakresie ochrony przed działaniem szkodliwego oprogramowania,
- ➔ metod uwierzytelnienia i autoryzacji w systemach informatycznych.

AUDYTY I SZKOLENIA

Audyt bezpieczeństwa danych osobowych obejmuje:

- identyfikację zbiorów danych osobowych przetwarzanych w organizacji,
- analizę i ocenę zgodności z wymaganiami Ustawy o ochronie danych osobowych,
- weryfikację poprawności stosowanych zabezpieczeń dla zbiorów danych osobowych - strona techniczna i organizacyjna,
- sporządzenie dokumentacji systemu zabezpieczeń zbiorów, zgodnej z wymaganiami rozporządzenia MSWiA,
- przygotowanie stosownych dokumentów do GIODO.



Wykres.

Ryzyko systemu po wdrożeniu środków zaradczych (Oprogramowanie Riscare)

- przed wdrożeniem
- po wdrożeniu

Analiza ryzyka obejmuje:

- identyfikowanie i klasyfikowanie aktywów, analizowanie zagrożeń, podatności oraz ryzyk systemu,
- ocenę doboru i wdrożenia zabezpieczeń w powiązaniu z wynikami analizy ryzyka,
- opracowanie lub współdziałanie w tworzeniu polityki i procedur bezpieczeństwa dla systemu informacyjnego.

BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH

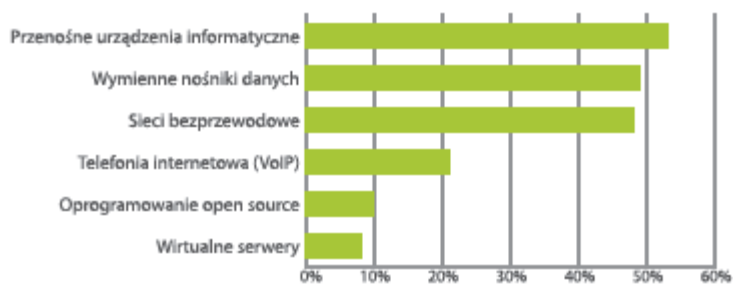


AUDYTY I SZKOLENIA

Audyt bezpieczeństwa fizycznego obejmuje:

- ➔ analizę i ocenę skuteczności istniejących rozwiązań zabezpieczeń fizycznych, ze wskazaniem na ich zgodność z wymaganiami ISO/IEC 27001:2005 oraz wymaganiami wynikającymi z ustawy o ochronie informacji niejawnej,
- ➔ współdziałanie w tworzeniu zabezpieczeń technicznych i organizacyjnych zgodnych z obowiązującymi regulacjami prawnymi i normatywnymi.

Wykres. Istotne zagrożenia dla bezpieczeństwa informacji



Szkolenia:

- ➔ szkolenia w zakresie bezpieczeństwa eksploatacji systemów informatycznych,
- ➔ szkolenia dotyczące ochrony danych osobowych w organizacji,
- ➔ szkolenia z analizy ryzyka,
- ➔ szkolenia w zakresie wdrażania i eksploatacji zabezpieczeń fizycznych systemów informacyjnych,
- ➔ szkolenia w zakresie zaawansowanych technologii zabezpieczeń systemów informatycznych.

BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH



AUDYTY I SZKOLENIA

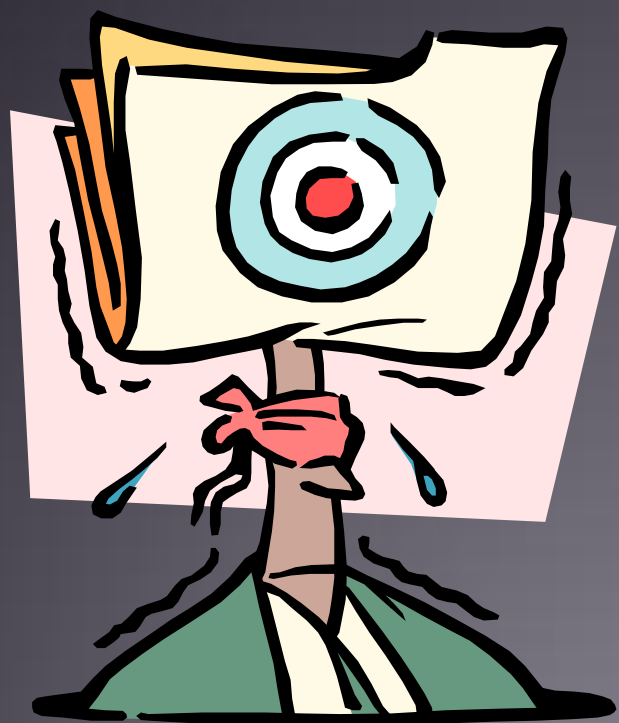
Audyty i szkolenia przeprowadzane we współpracy z pracownikami Laboratorium Certyfikacji Produktów i Systemów Informatycznych Wydziału Informatyki Zachodniopomorskiego Uniwersytetu Technologicznego.

KONTAKT:

**Oddział Regionalny
Szczecińskiego Parku Naukowo-Technologicznego
z siedzibą w Bydgoszczy**
ul. 62 Pułku Piechoty Wielkopolskiej 6
85-825 Bydgoszcz

Mariusz Andryszak
Dyrektor Oddziału Regionalnego SPNT w Bydgoszczy
tel. 797 599 363
mandryszak@spnt.pl
www.spnt.pl





Dziękuję Państwu
za uwagę!

Pytania?