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**)

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 wypowiadana 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 osiągania 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.

10.05.2011

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”;

10.05.2011

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

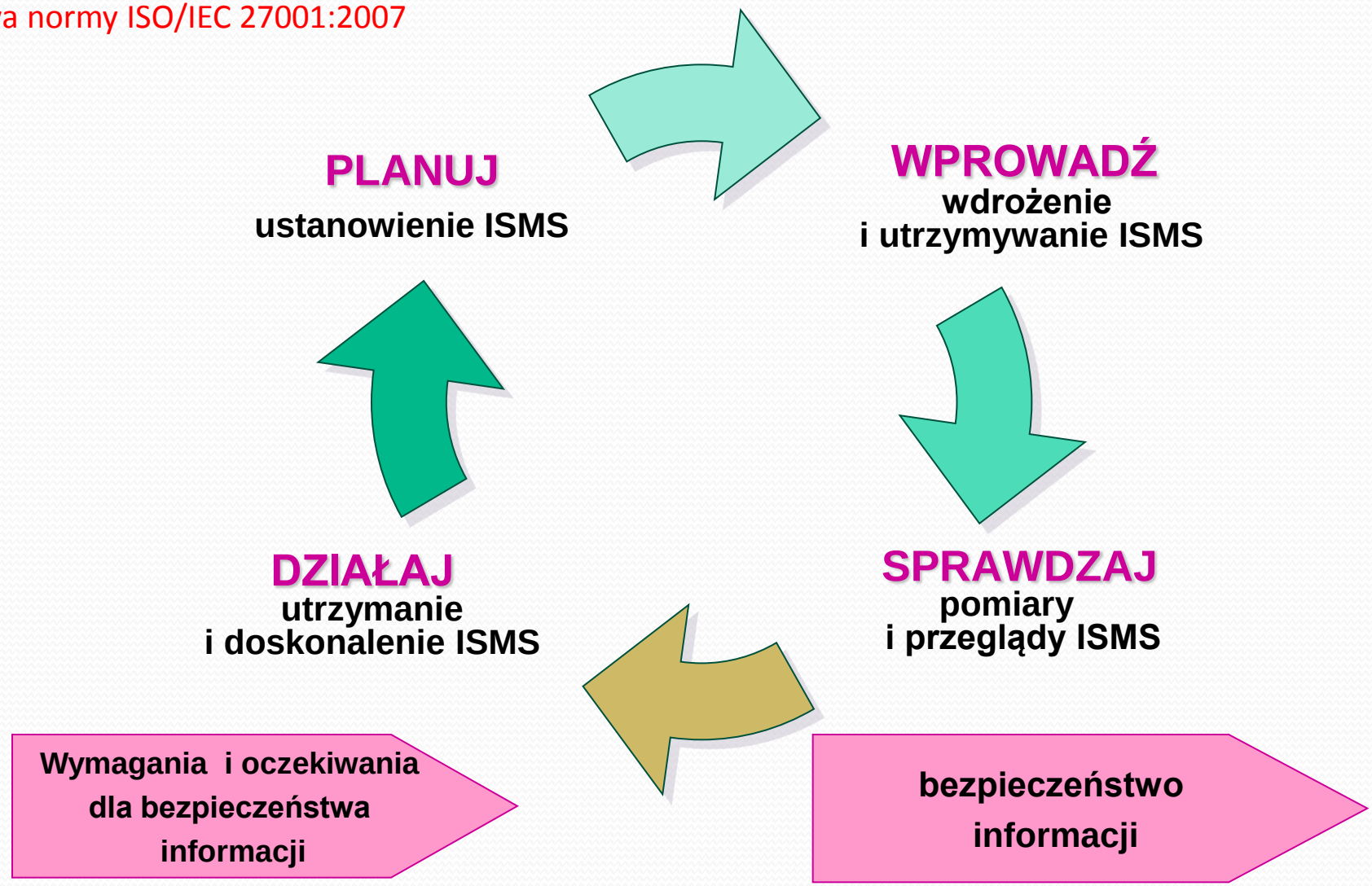
System zarządzania bezpieczeństwem informacji (ISMS - ZBSI)

- 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

Według: *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.

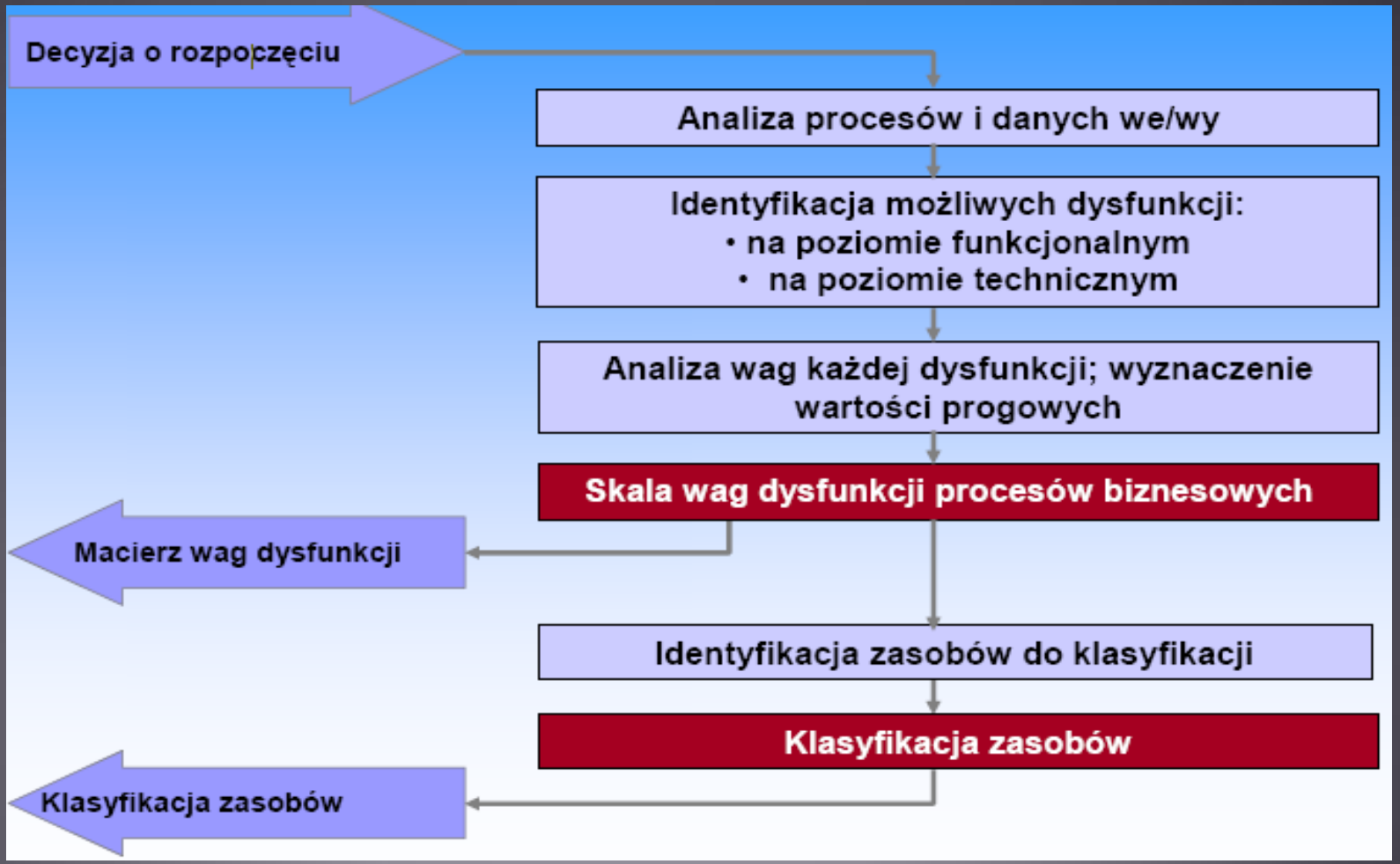
→ **Utrzymywanie przyjętego poziomu bezpieczeństwa**

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 configuracyjnych 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 źrodłowe 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 prawnimi (np. Ustawami) odnośnie ochrony życia i prywatności personelu	2		
C02	Niezgodność z prawem i regulacjami prawnimi (np. Ustawami) odnośnie kontroli finansowej	2		
C03	Niezgodność z prawem i regulacjami prawnimi (np. Ustawami) odnośnie wlsności intelektualnej	3		
C04	Niezgodność z prawem i regulacjami prawnimi (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 prawdopodobieństwa zdarzeń / Oszacowanie podatności		P=1 Bardzo niskie	P=2 Niskie	P=3 możliwe	P=4 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

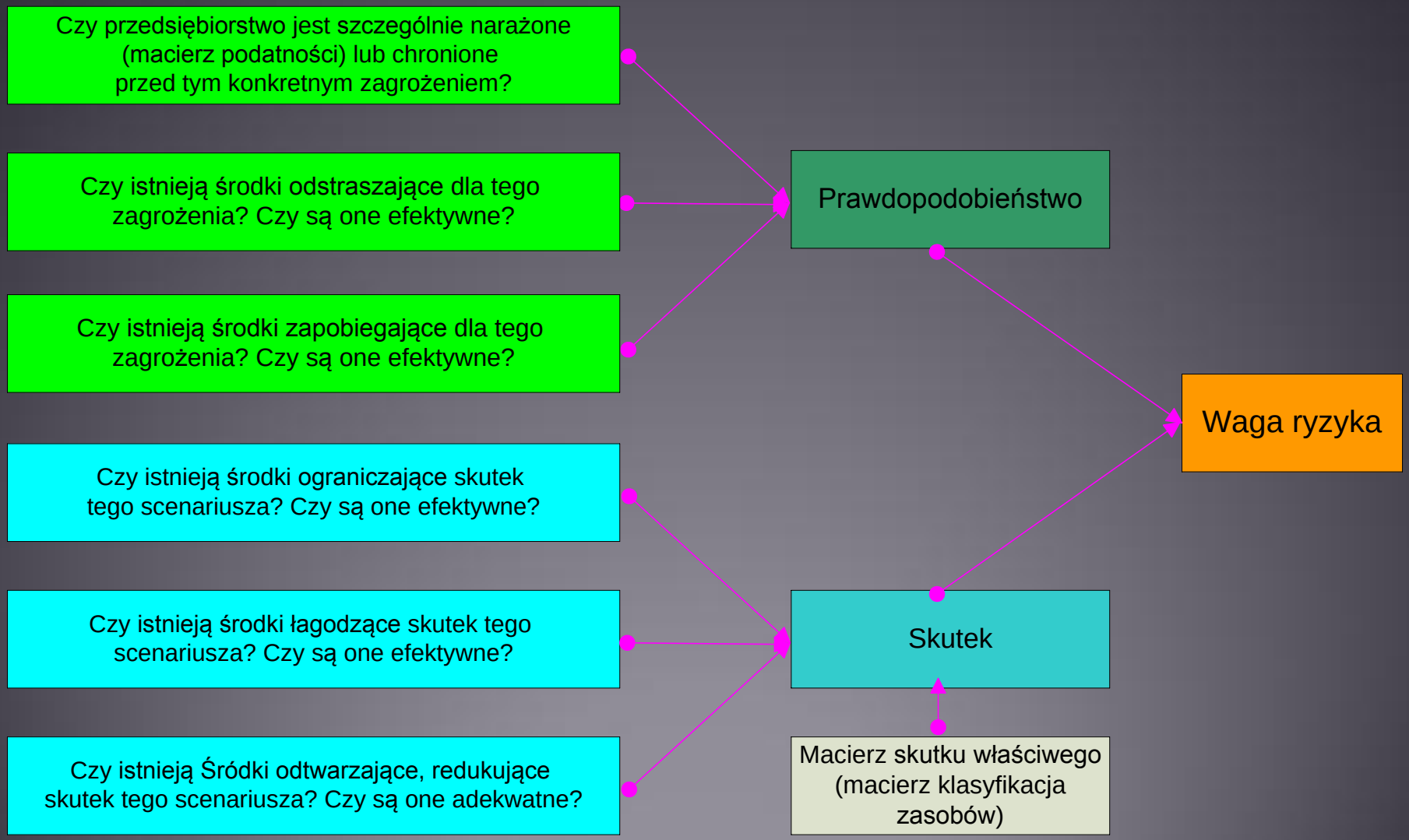
Etap III - Scenariusze zagrożeń

Skojarzenie zasobów z podatnościami

Scenariusz				Zasoby	Podatność
	Przyczyna				
		Pochodzenia : rodzaj ataku i/lub czynność			
01	Przejściowa 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

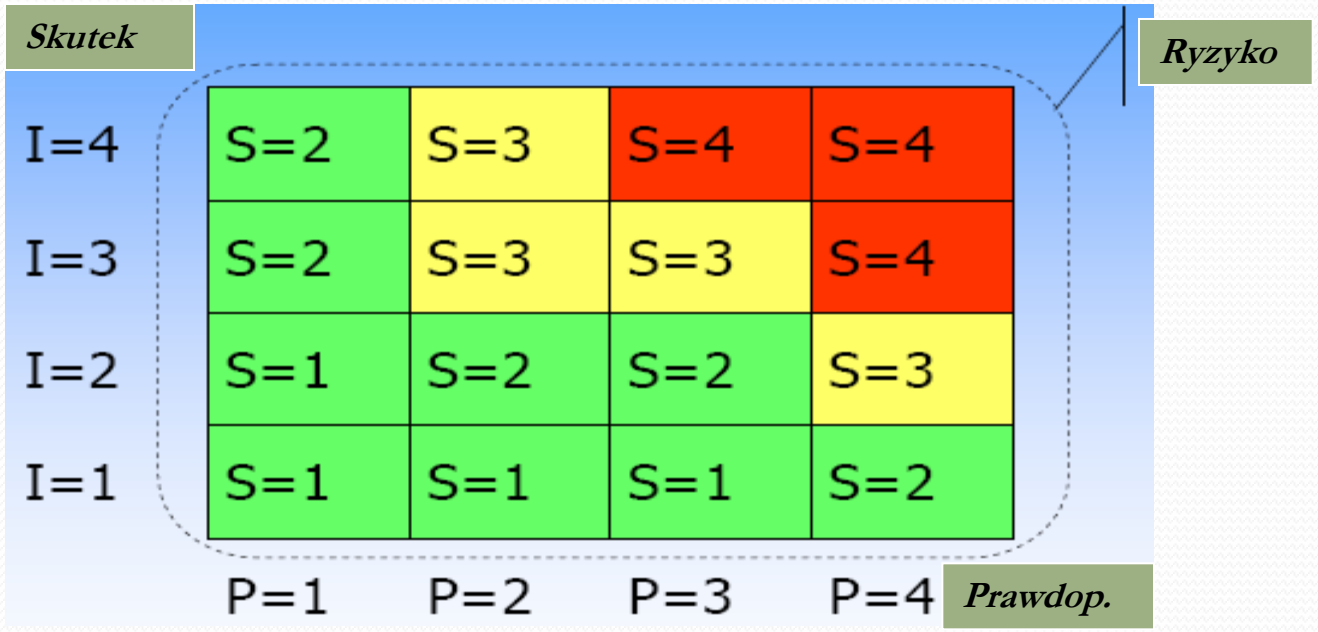
Proces analizy scenariusza zagrożenia



Analiza Ryzyka

Przykładowa macierz akceptacji ryzyka

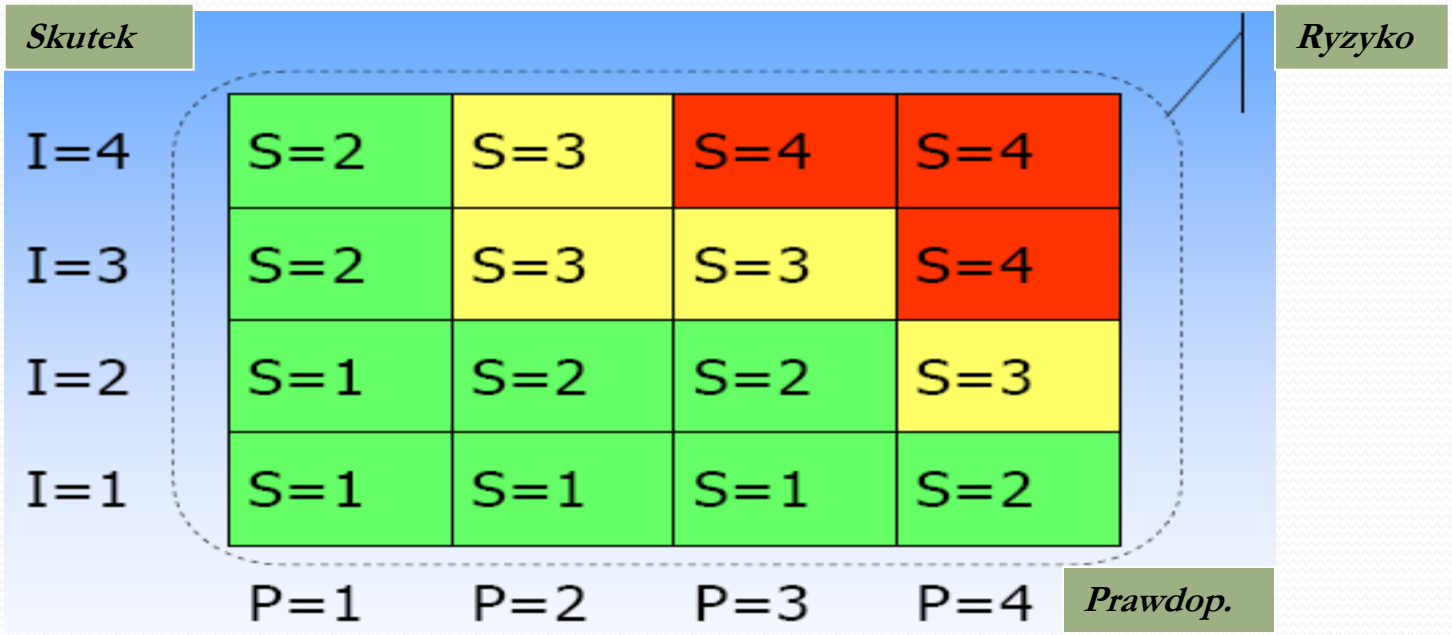
- **Waga scenariusza zagrożenia jest funkcją jego prawdopodobieństwa oraz skutku. Otrzymaną macierz nazywamy macierzą akceptacji ryzyka, która definiuje akceptowalność ryzyka w funkcji jego szacowanego prawdopodobieństwa oraz skutku.**



Analiza Ryzyka

Macierz akceptacji ryzyka

- **Na macierzy akceptacji ryzyka wyróżnia się 3 kategorie ryzyk:**



- ✓ 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).

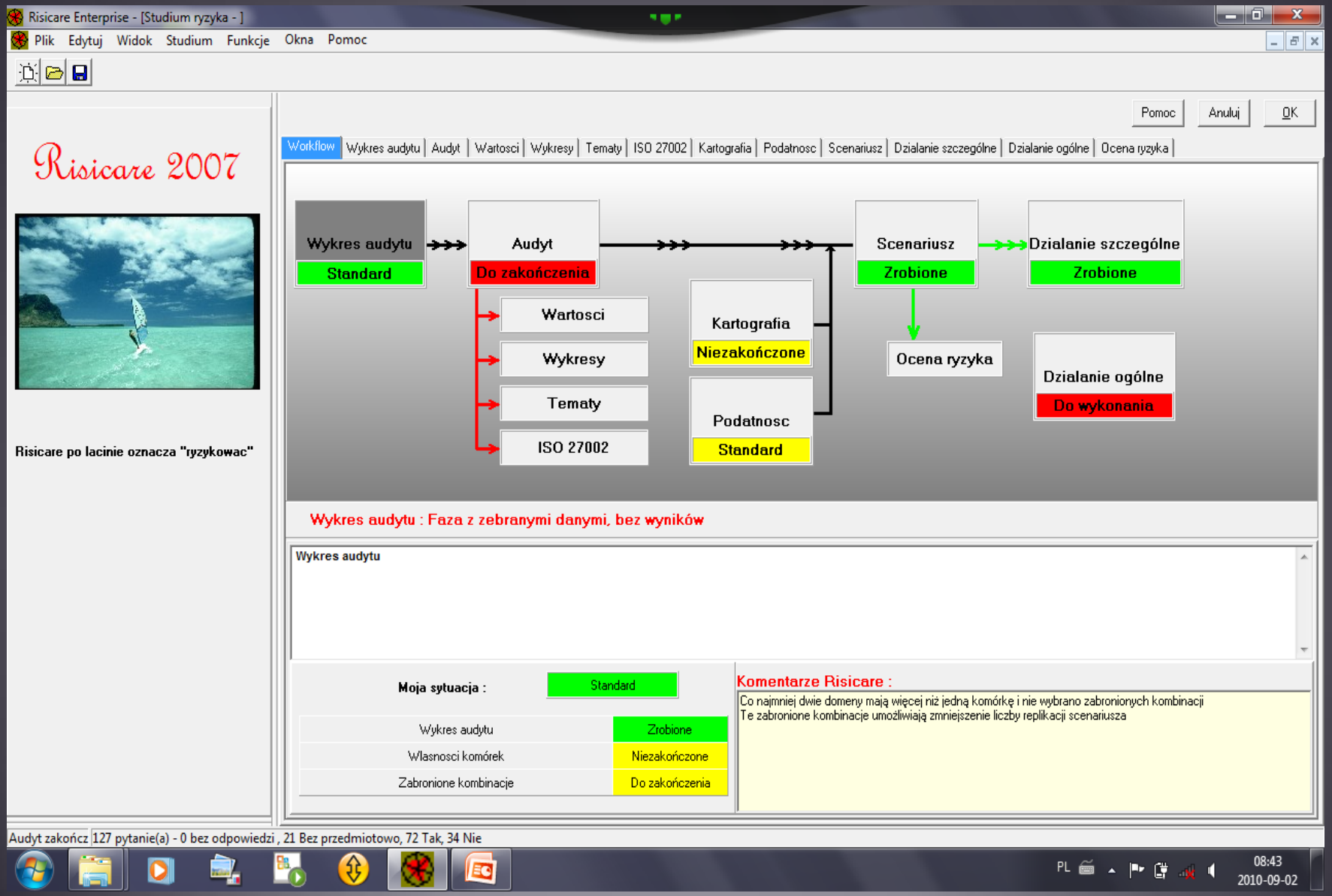
Analiza ryzyka

Oprogramowanie do analizy ryzyka „ Risicare” oparte na metodzie Mehari

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

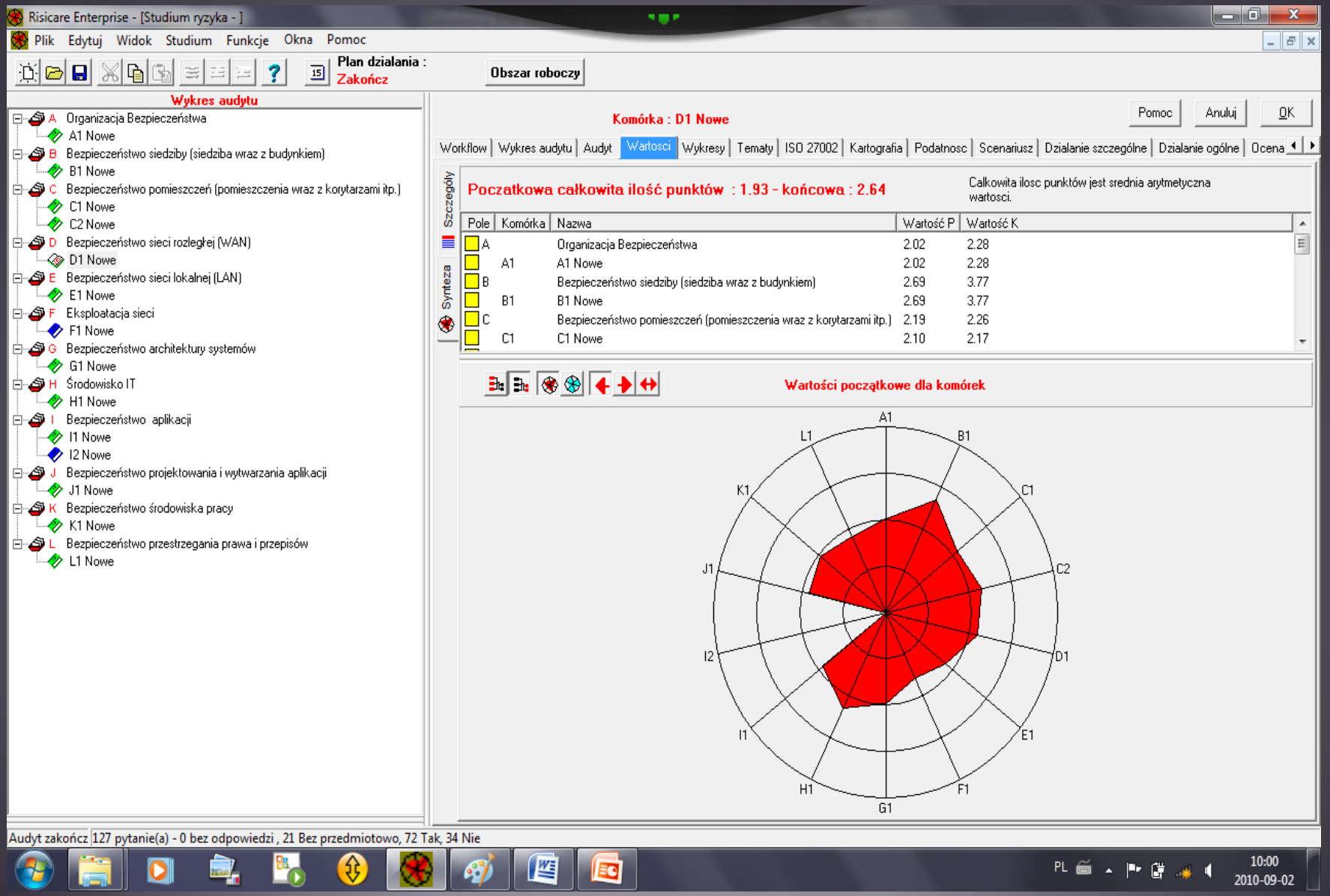
Etapy Analizy Ryzyka w/g. Mehari

Zrzut ekranu Risicare



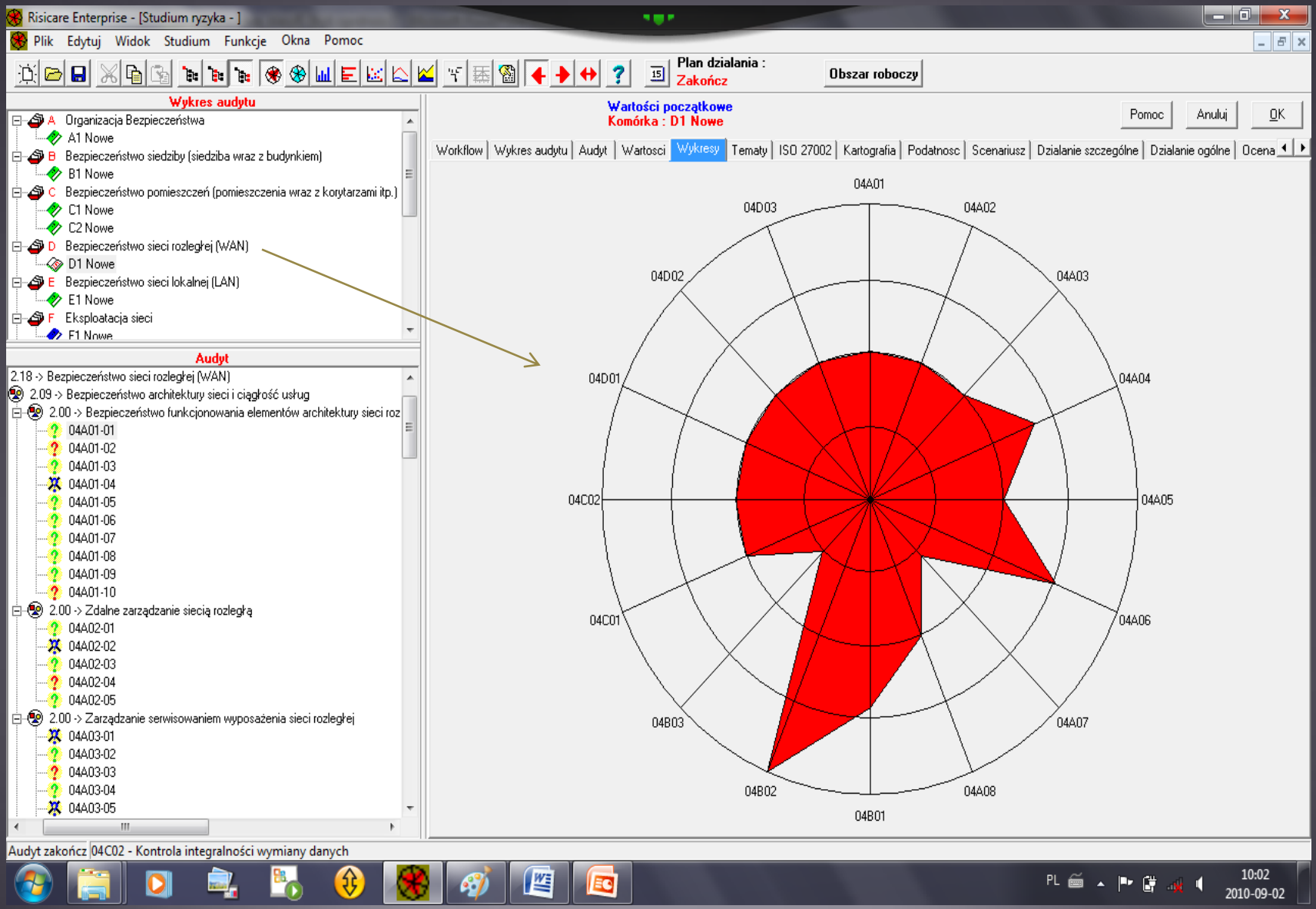
Etapy Analizy Ryzyka w/g. Mehari

Wyniki audytu dla wszystkich domen bezpieczeństwa



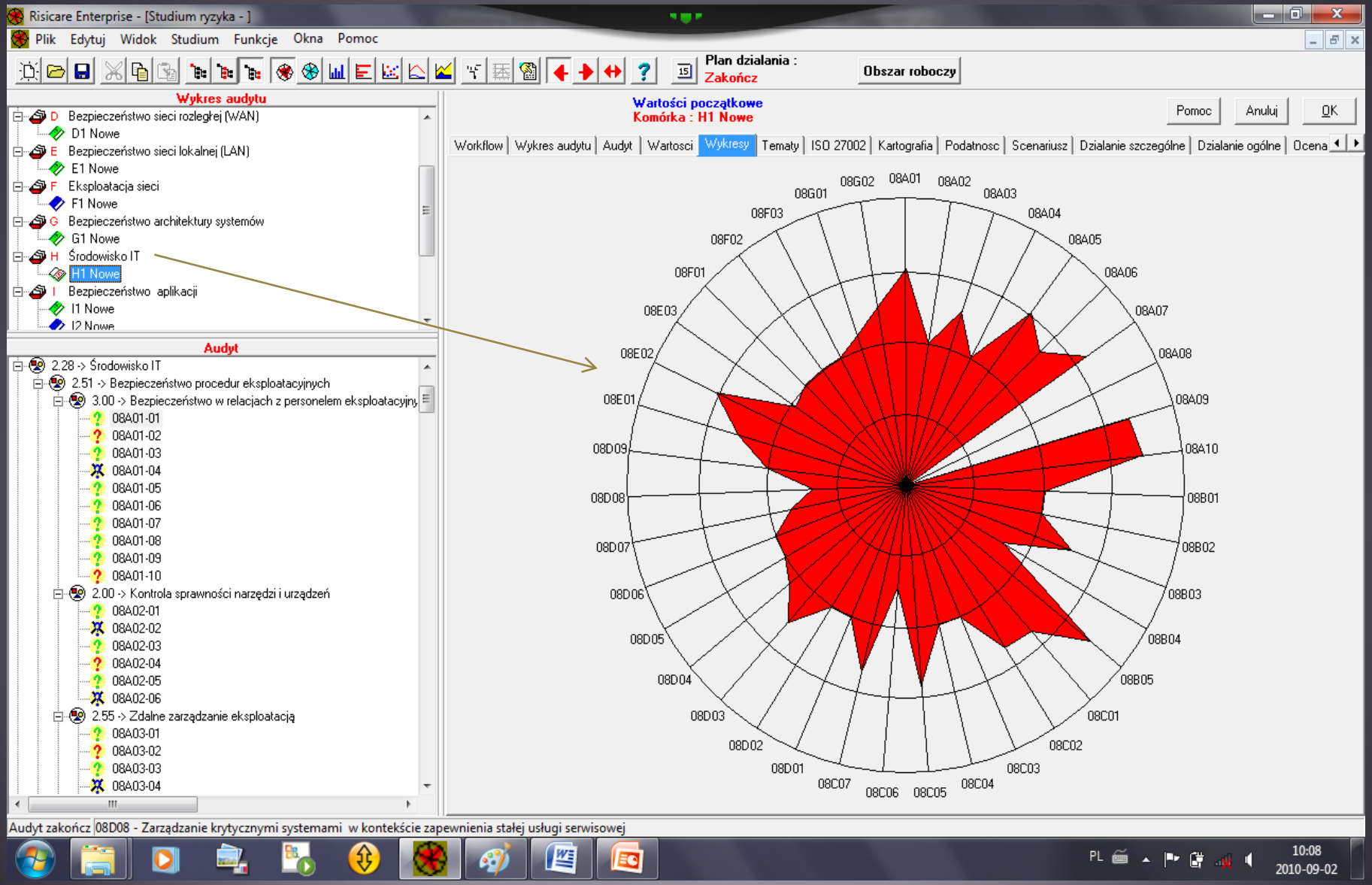
Etapy Analizy Ryzyka w/g. Mehari

Wynik audytu dla domeny bezpieczeństwa WLAN



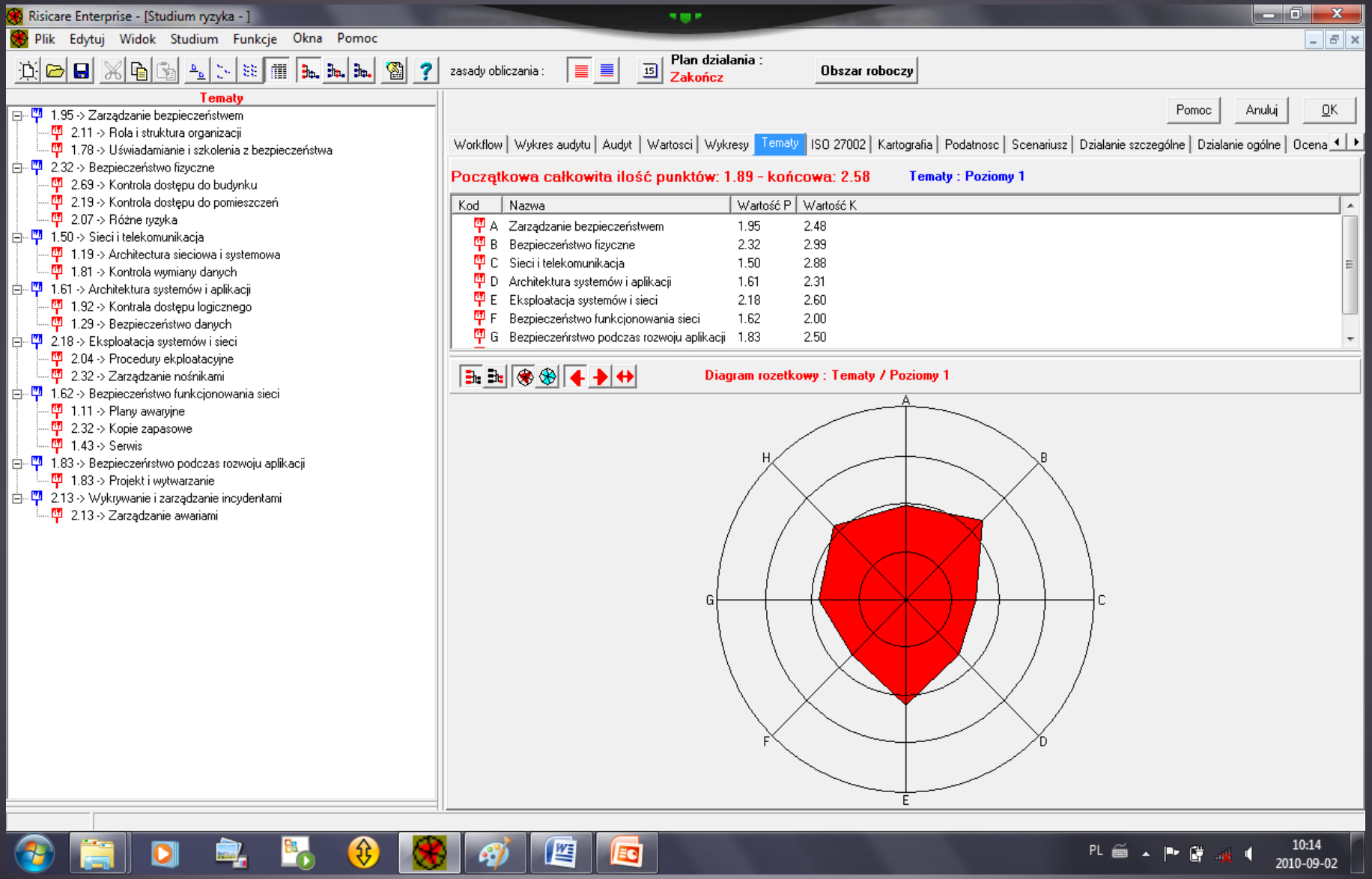
Etapy Analizy Ryzyka w/g. Mehari

Wynik audytu dla domena bezpieczeństwa środowiska IT



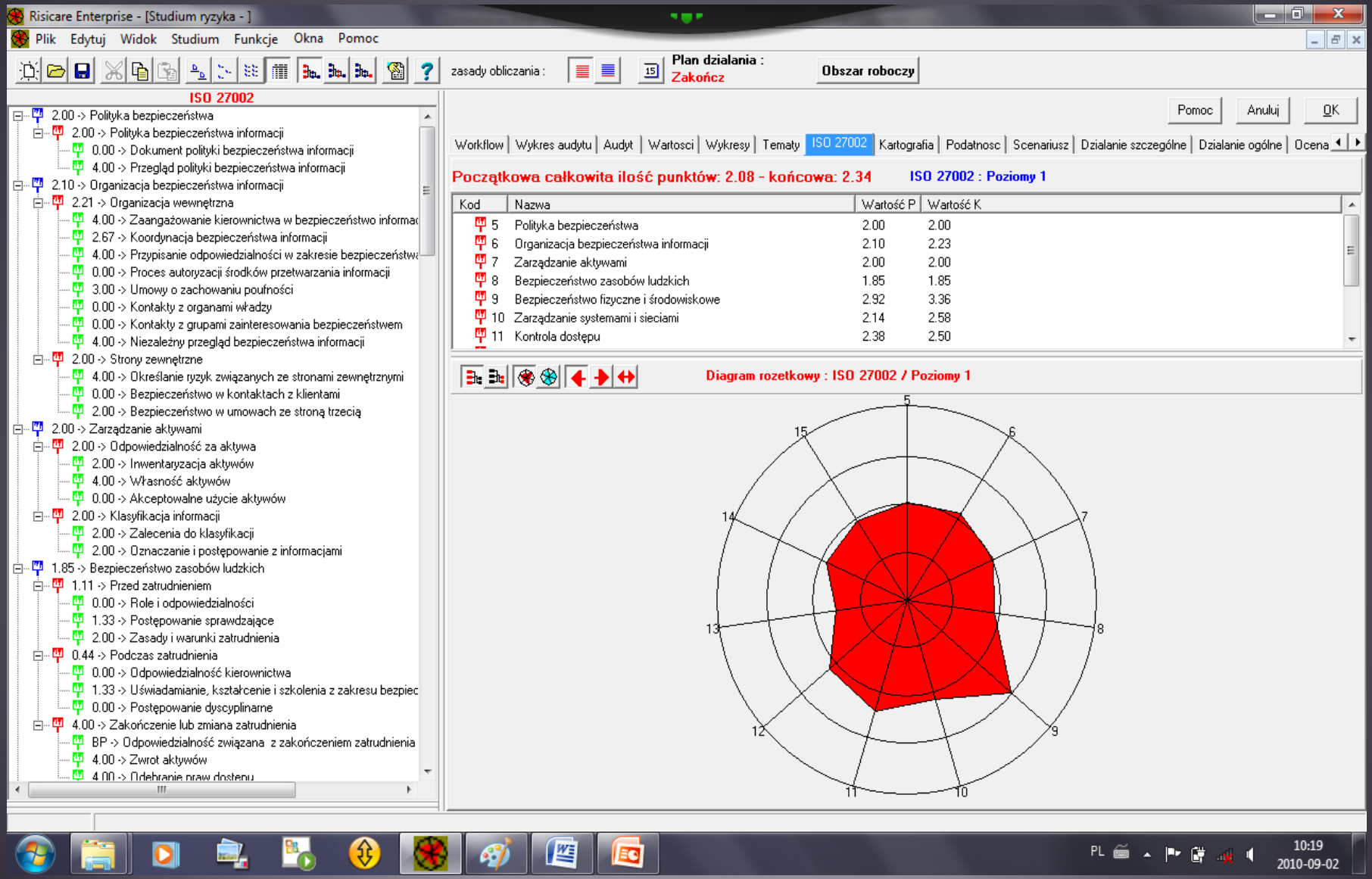
Etapy Analizy Ryzyka w/g. Mehari

Wynik audytu dla ważniejszych domen bezpieczeństwa



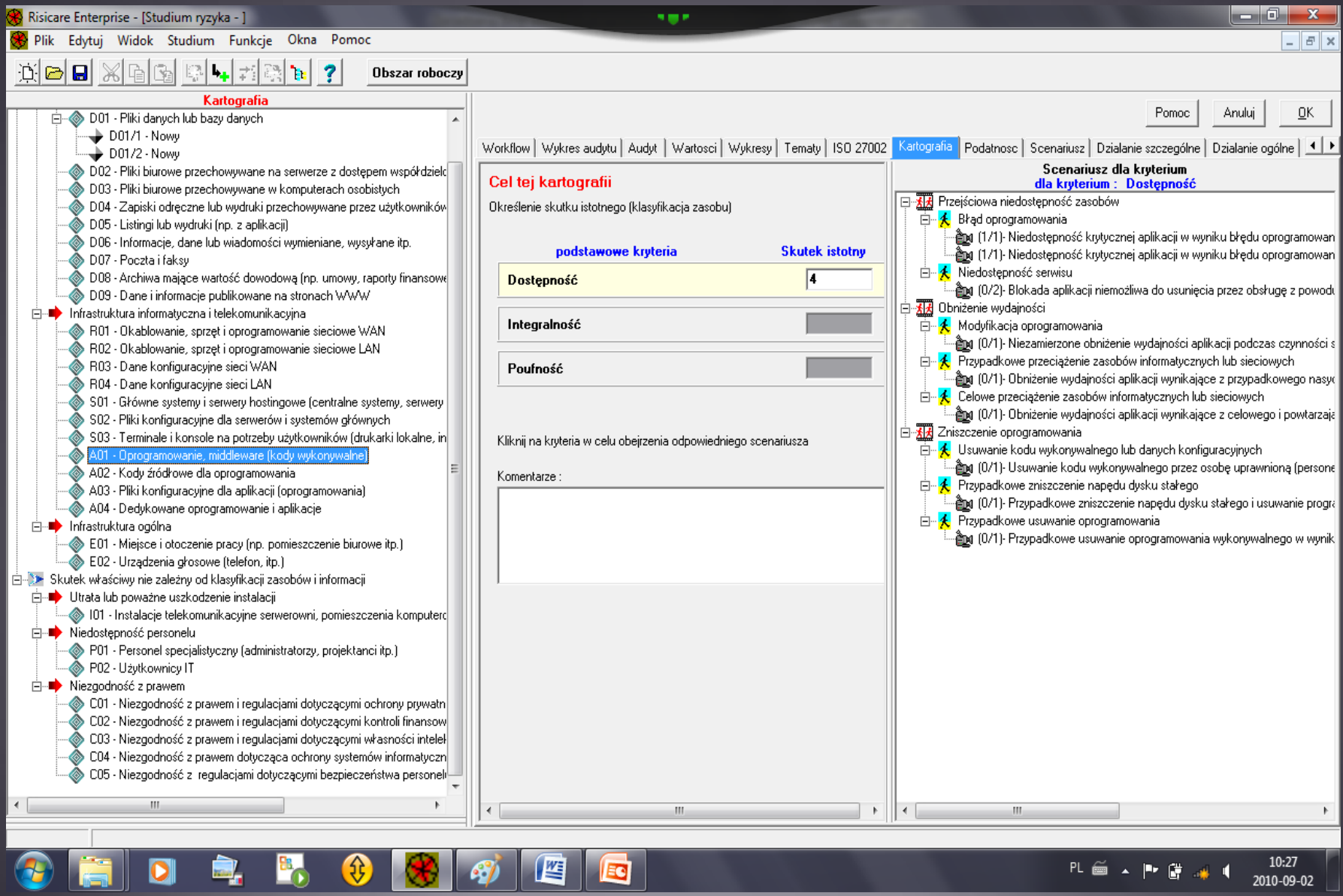
Etapy Analizy Ryzyka w/g. Mehari

Zgodność z ISO/IEC 27001



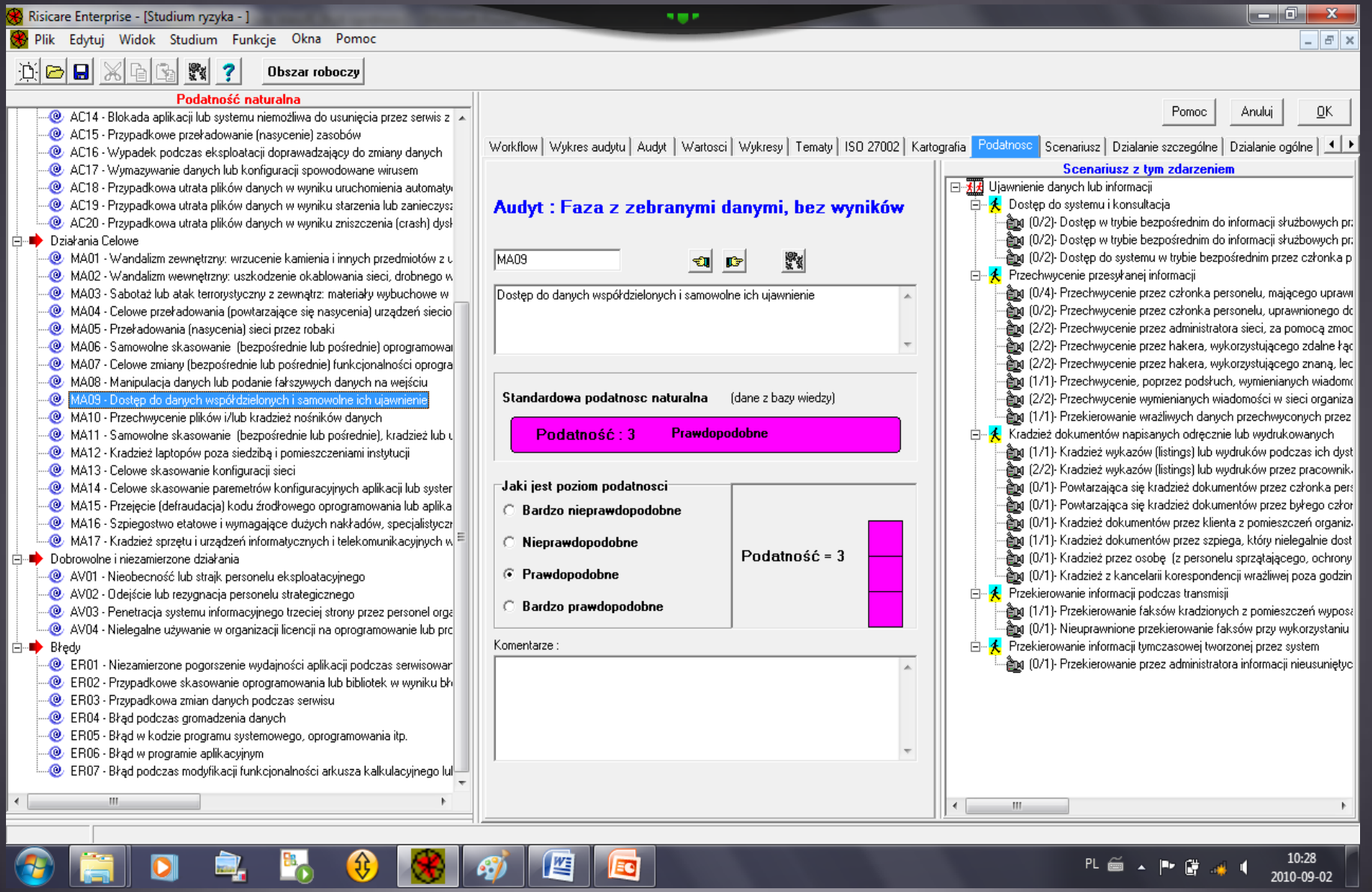
Etapy Analizy Ryzyka w/g. Mehari

Klasyfikacja zasobów



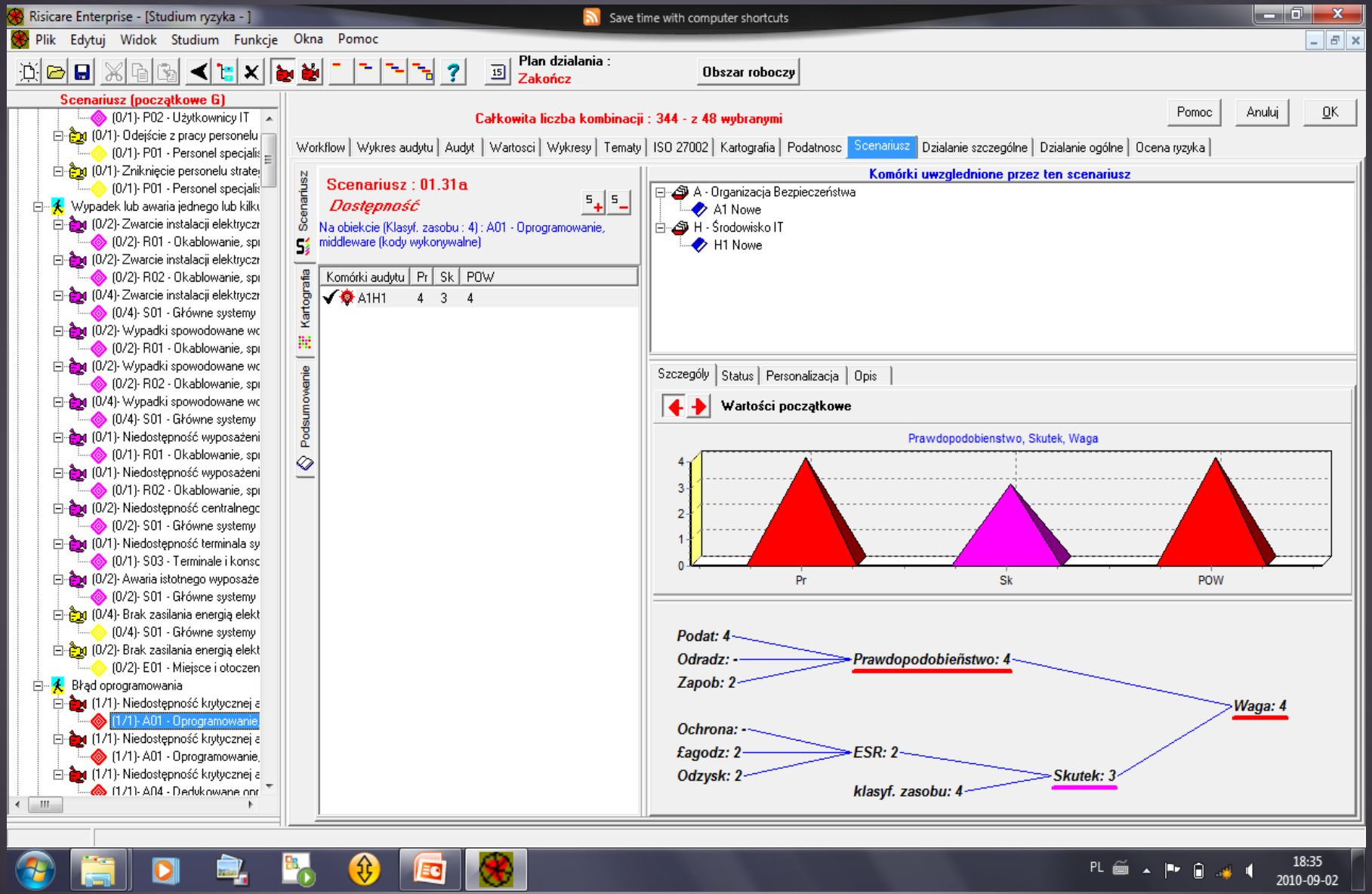
Etapy Analizy Ryzyka w/g. Mehari

Klasyfikacja podatności zasobów



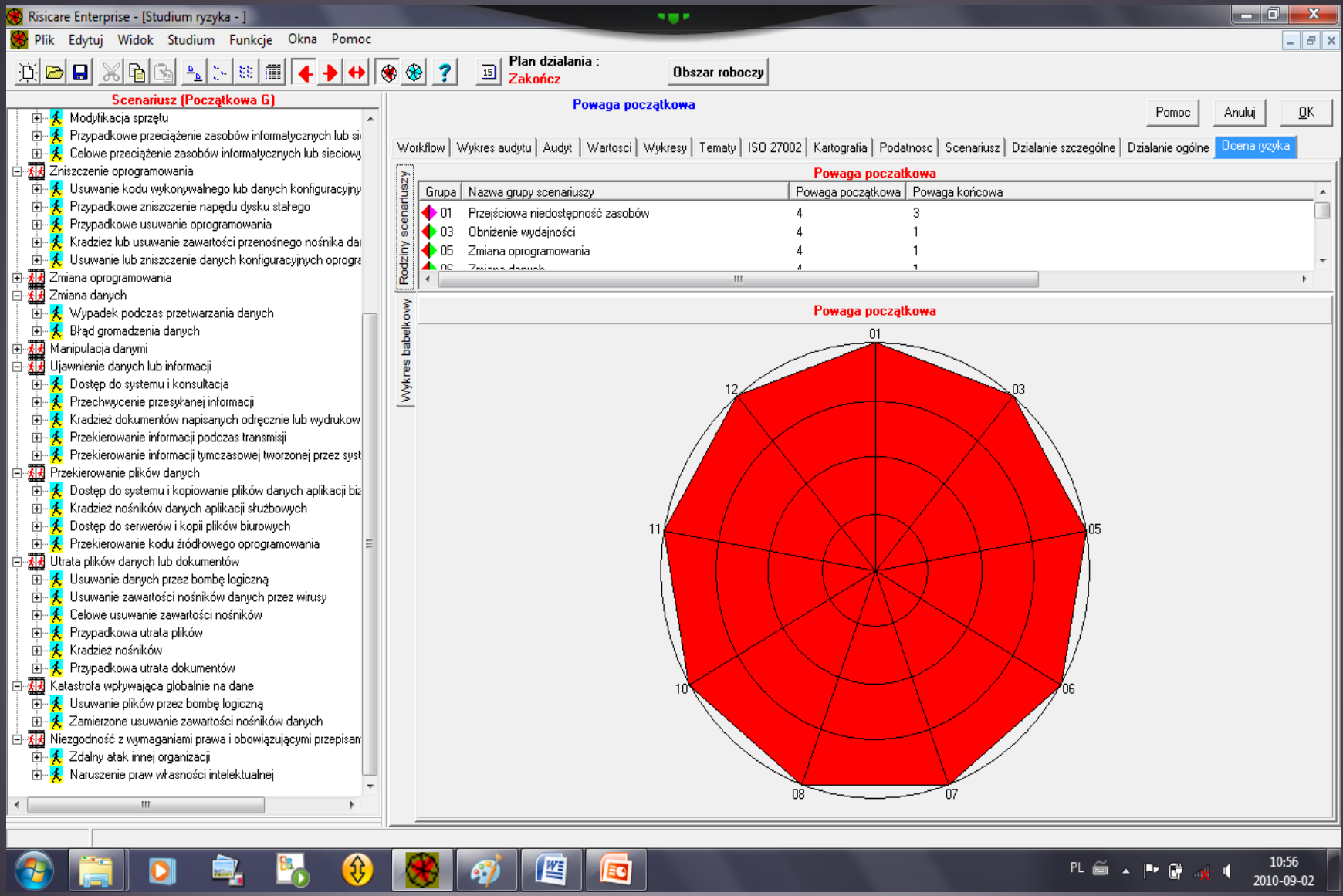
Etapy Analizy Ryzyka w/g. Mehari

Zobrazowane wyniki analizy ryzyka dla każdego ze scenariuszy zagrożeń



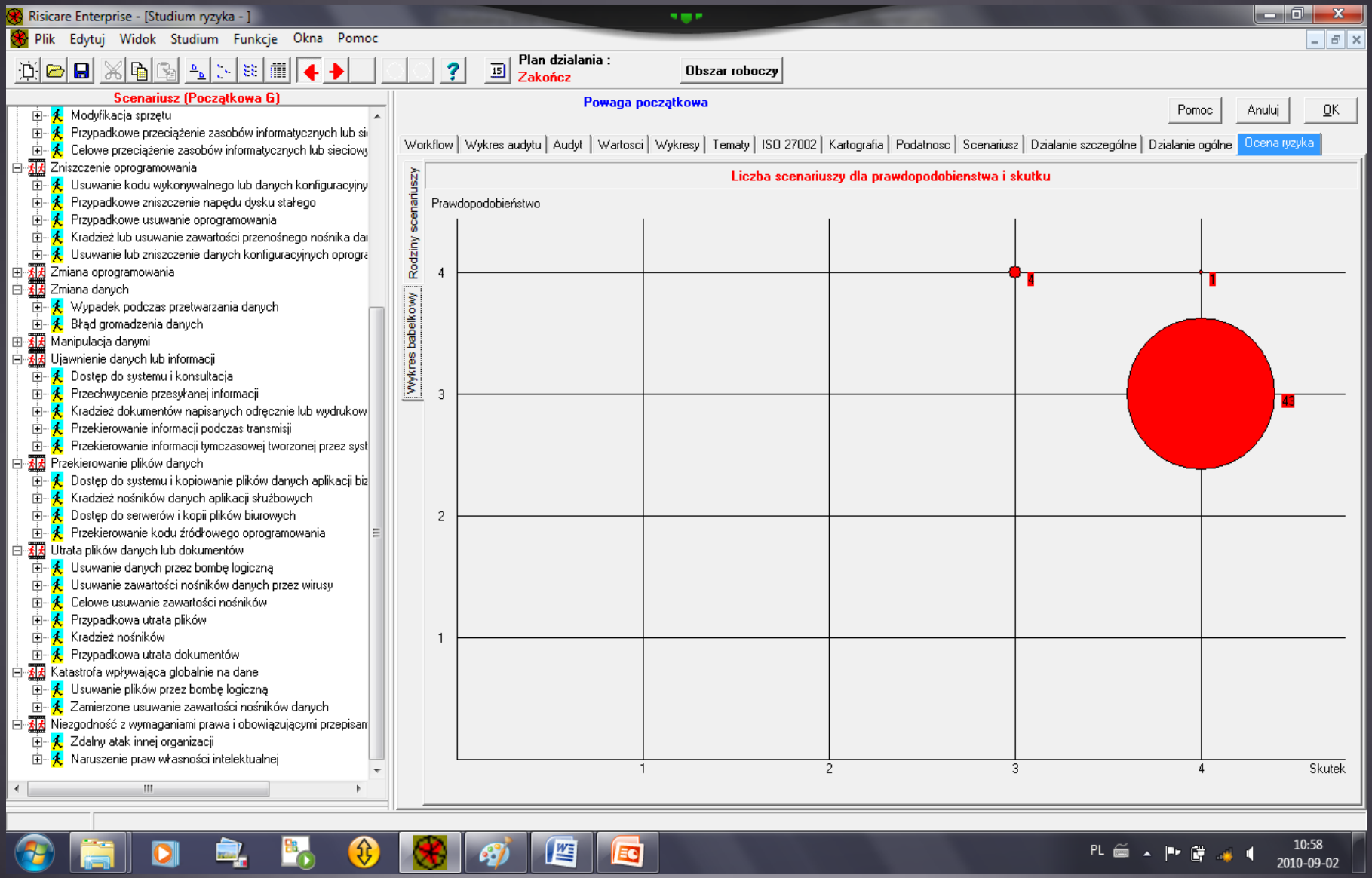
Etapy Analizy Ryzyka w/g. Mehari

Waga ryzyka dla wszystkich scenariuszy



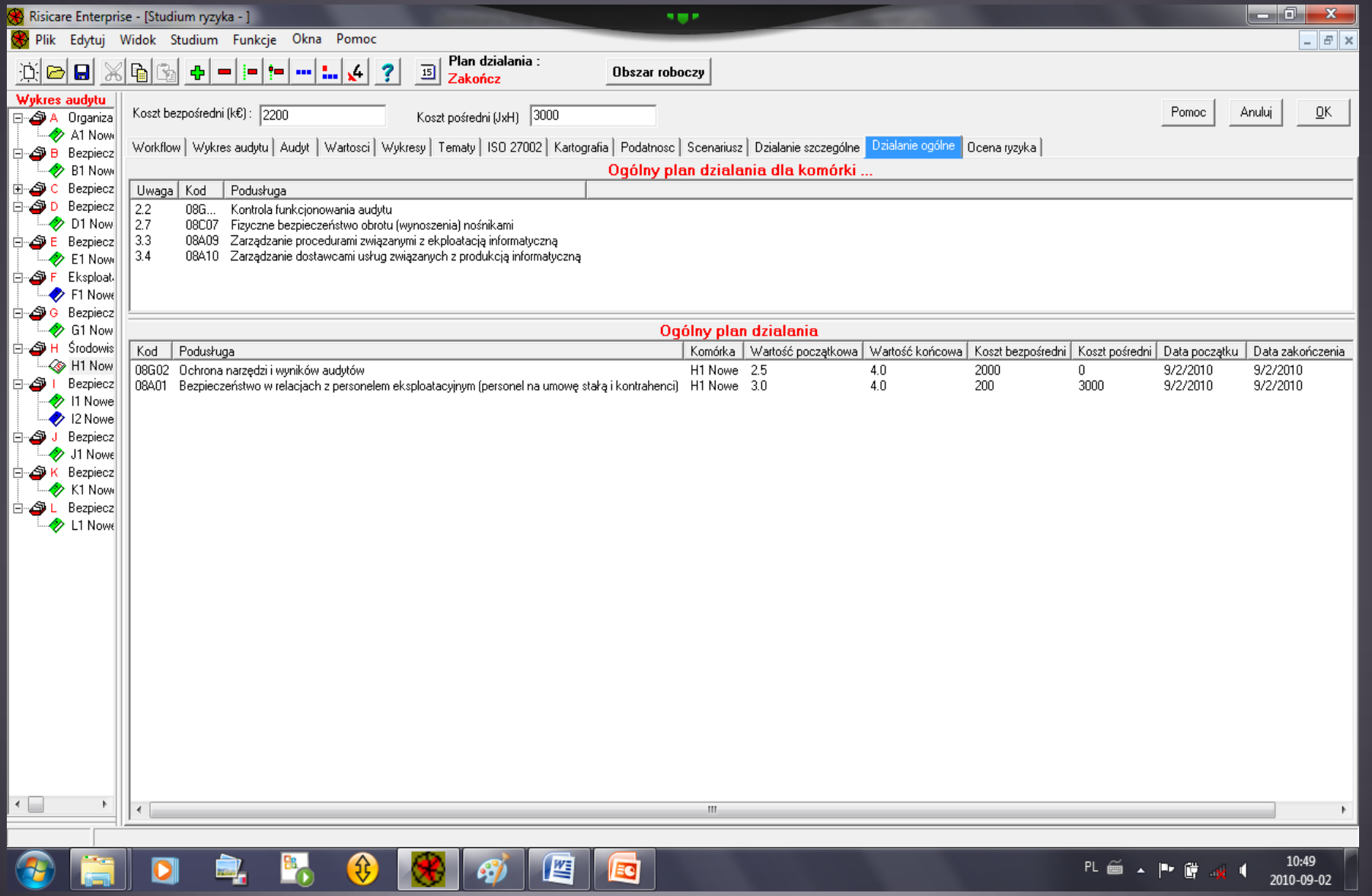
Etapy Analizy Ryzyka w/g. Mehari

Waga ryzyka dla wszystkich scenariuszy



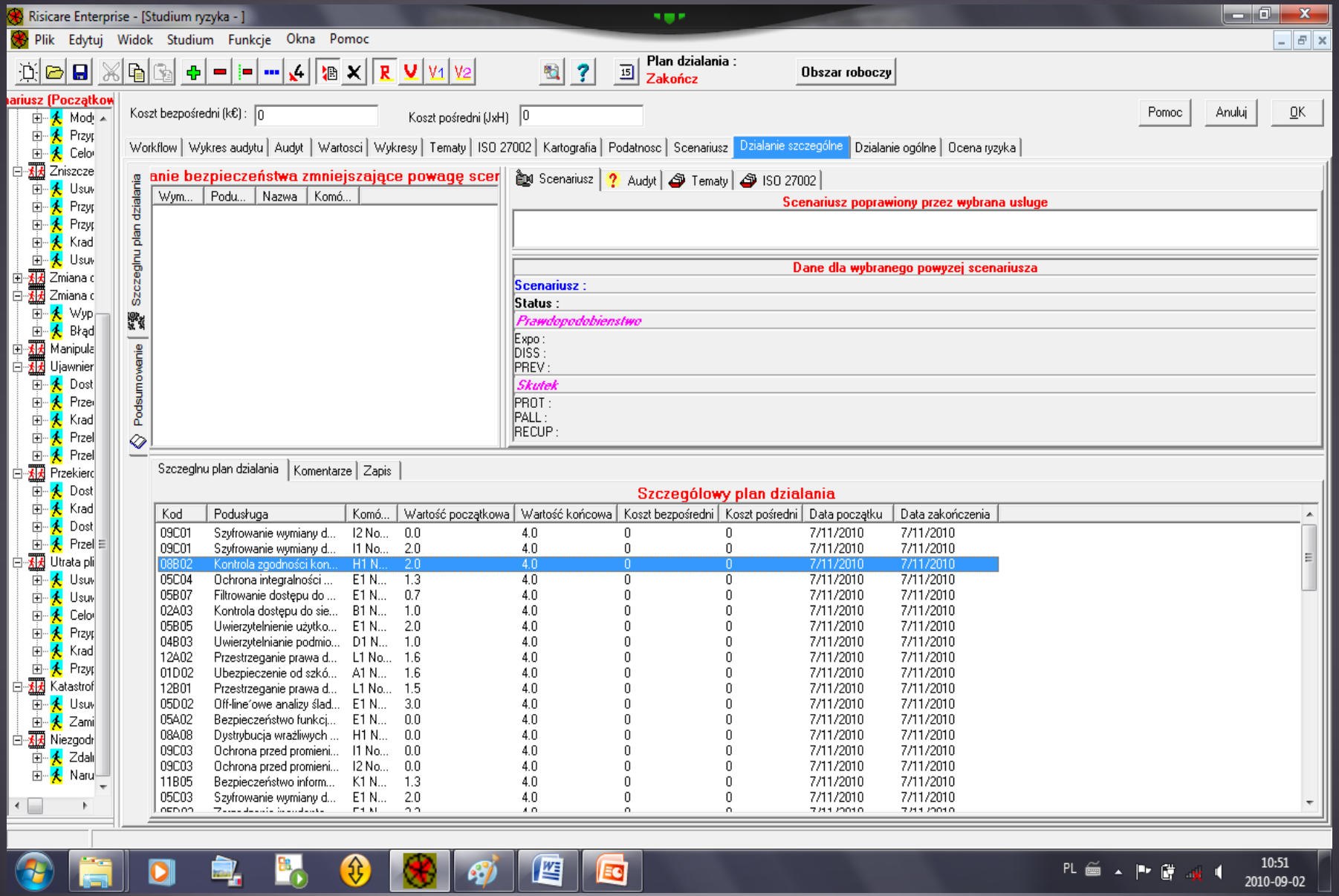
Etapy Analizy Ryzyka w/g. Mehari

Manualny interfejs wyboru środków zaradczych



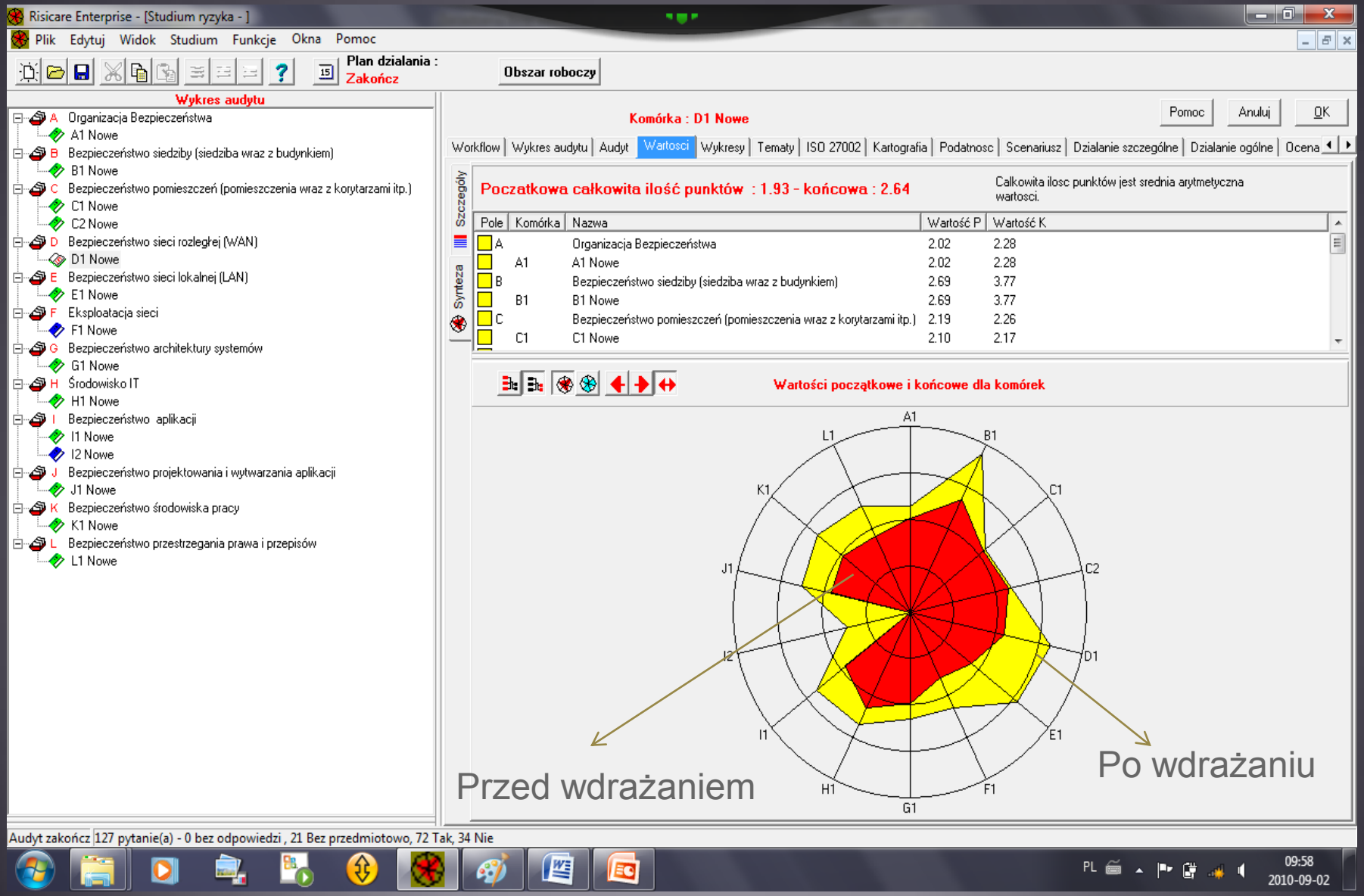
Etapy Analizy Ryzyka w/g. Mehari

Zautomatyzowany interfejs wyboru środków zaradczych



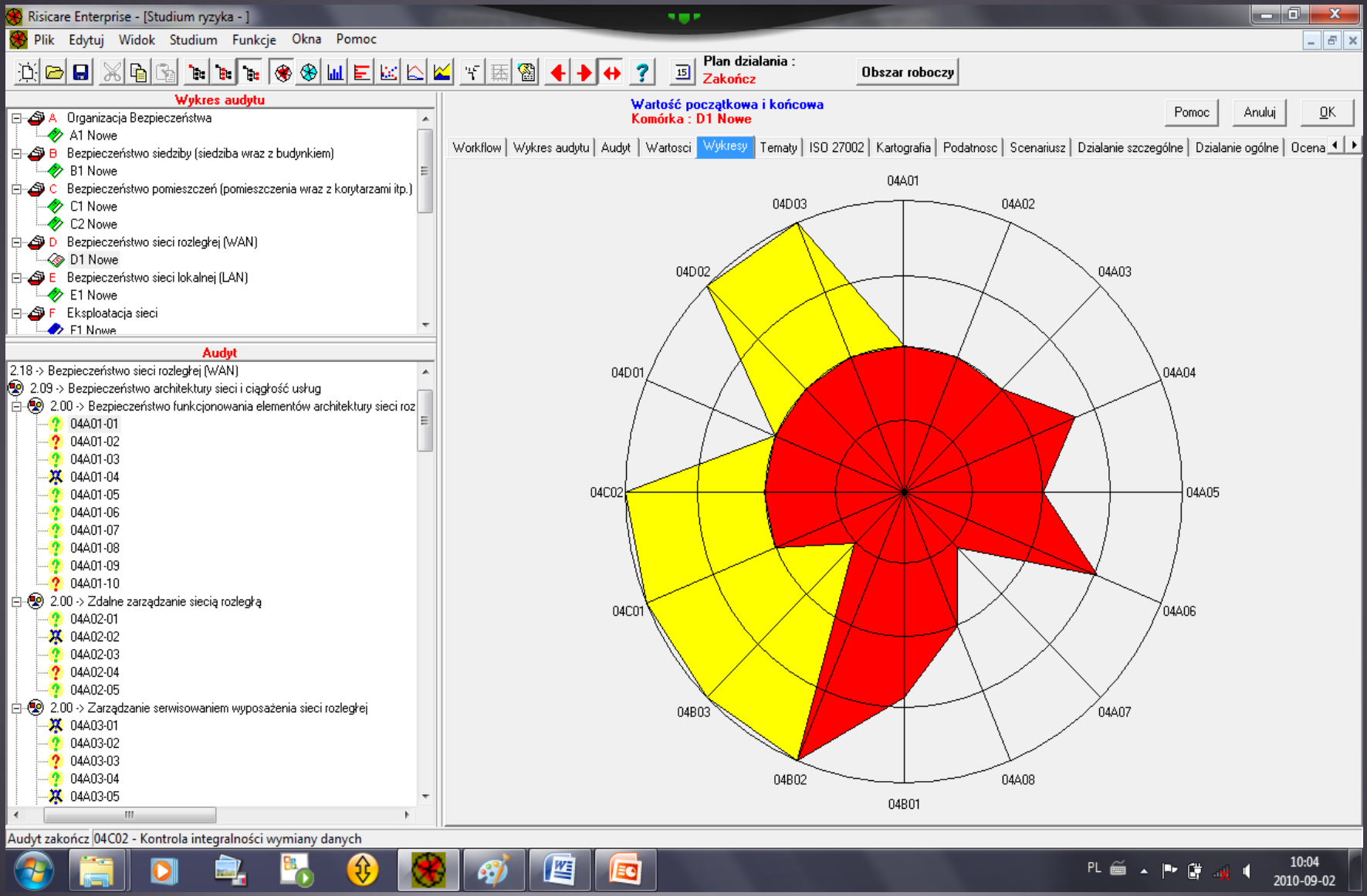
Etapy Analizy Ryzyka w/g. Mehari

Wyniki audytu dla domen bezpieczeństwa po wdrożeniu środków zaradczych



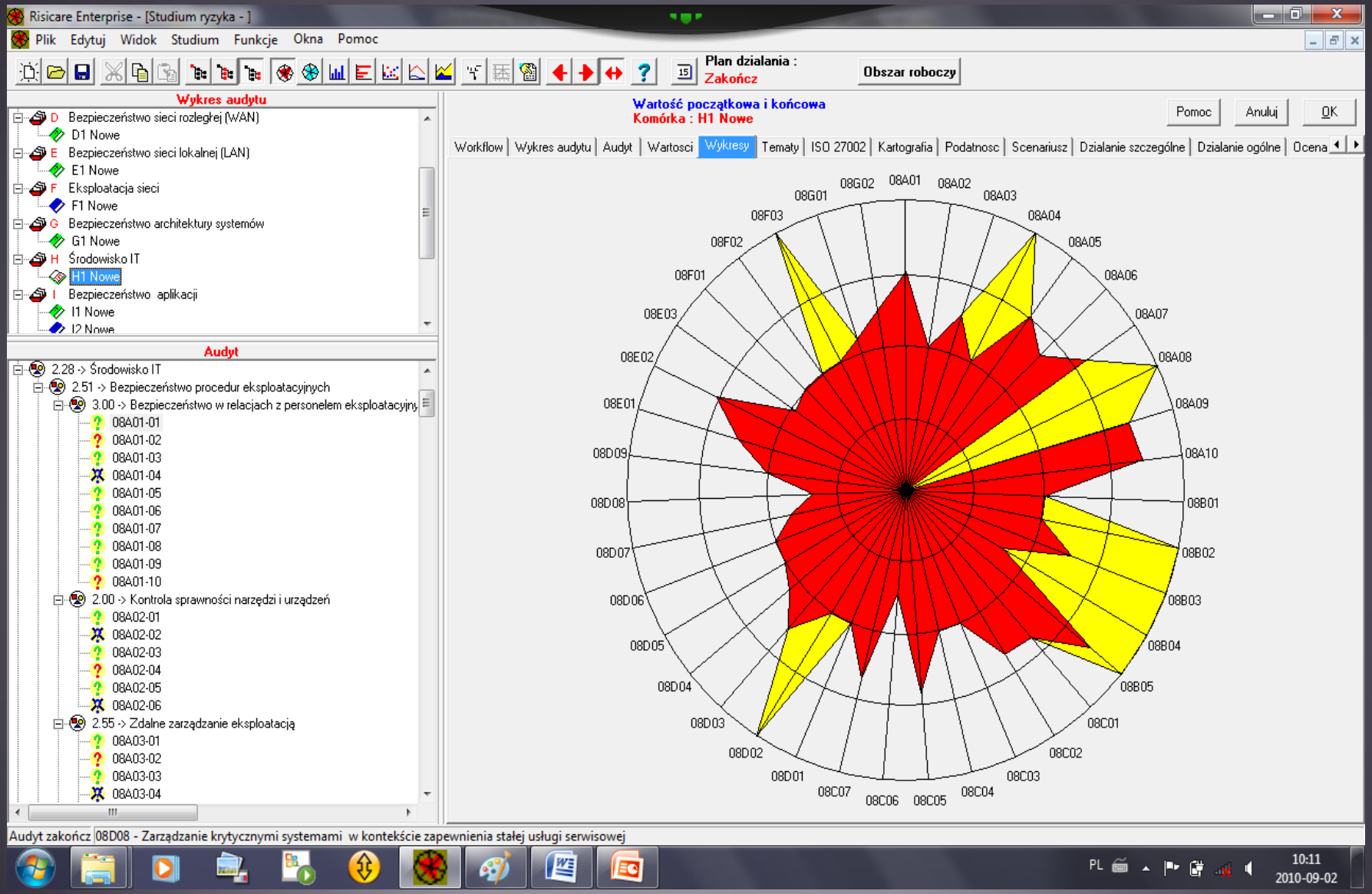
Etapy Analizy Ryzyka w/g. Mehari

Wyniki audytu dla WLAN'u po wdrożeniu środków zaradczych



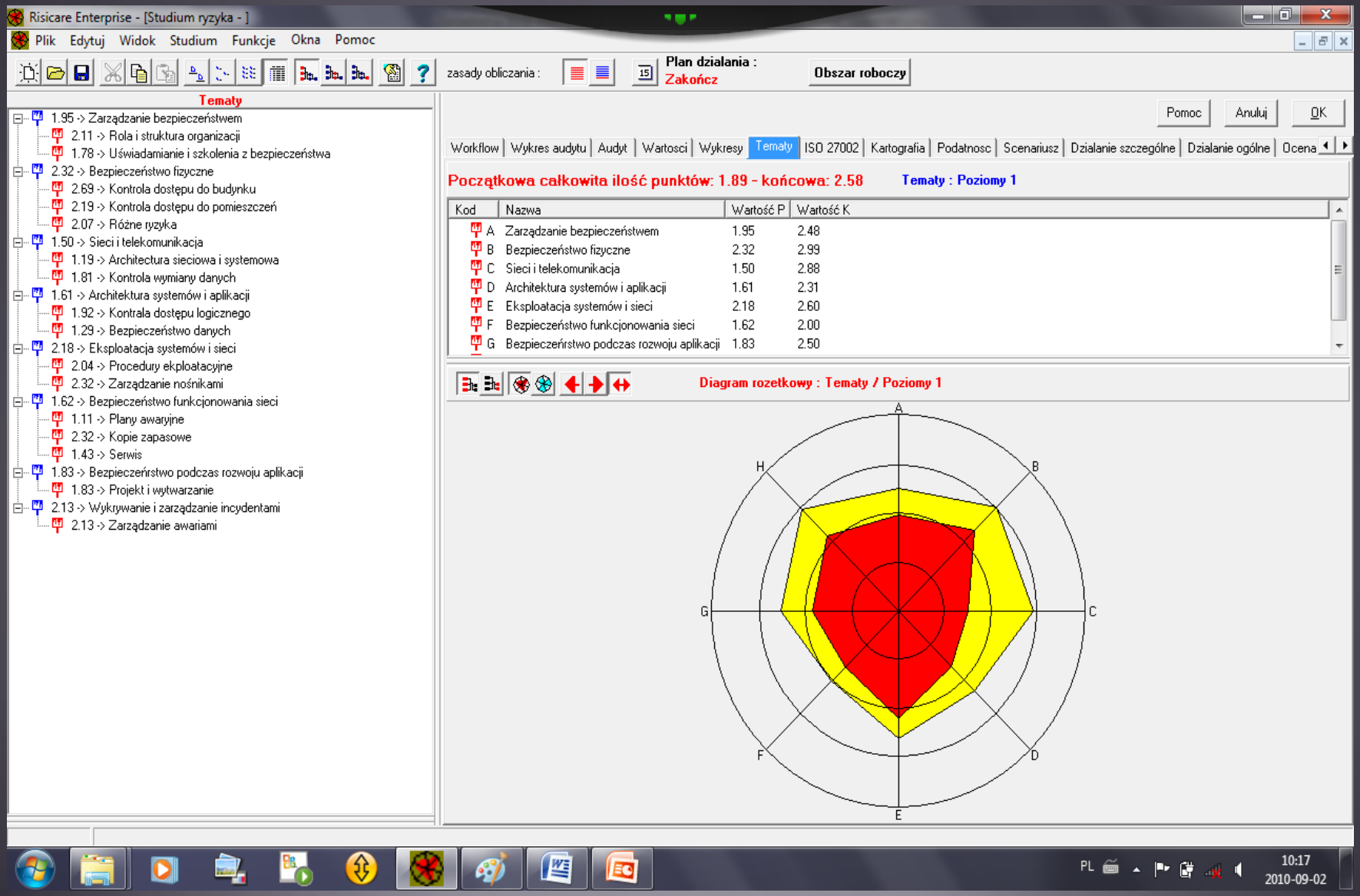
Etapy Analizy Ryzyka w/g. Mehari

Wyniki audytu dla środowiska IT po wdrożeniu środków zaradczych



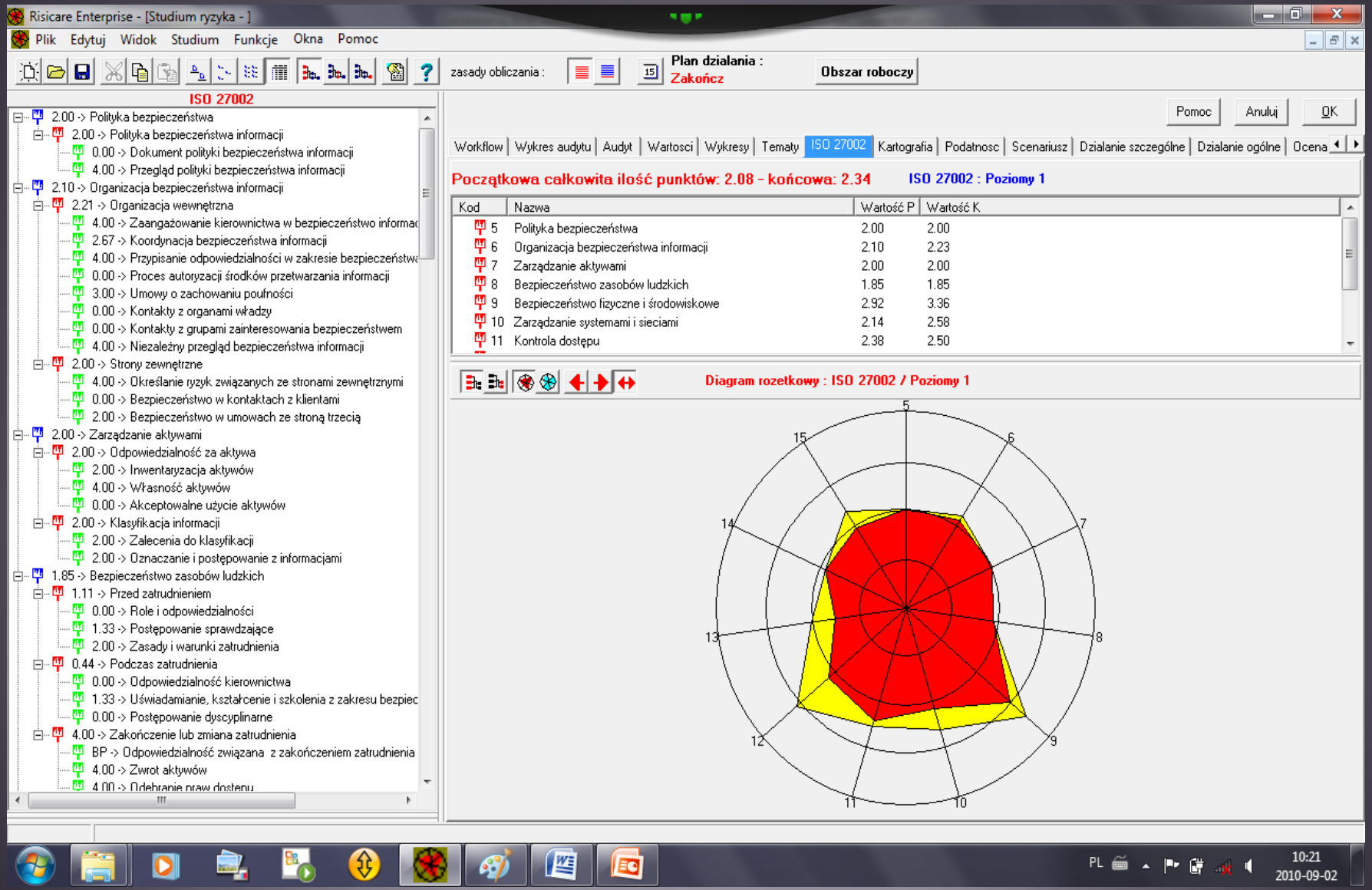
Etapy Analizy Ryzyka w/g. Mehari

Wynik audytu dla ważniejszych domen po wdrożeniu środków zaradczych



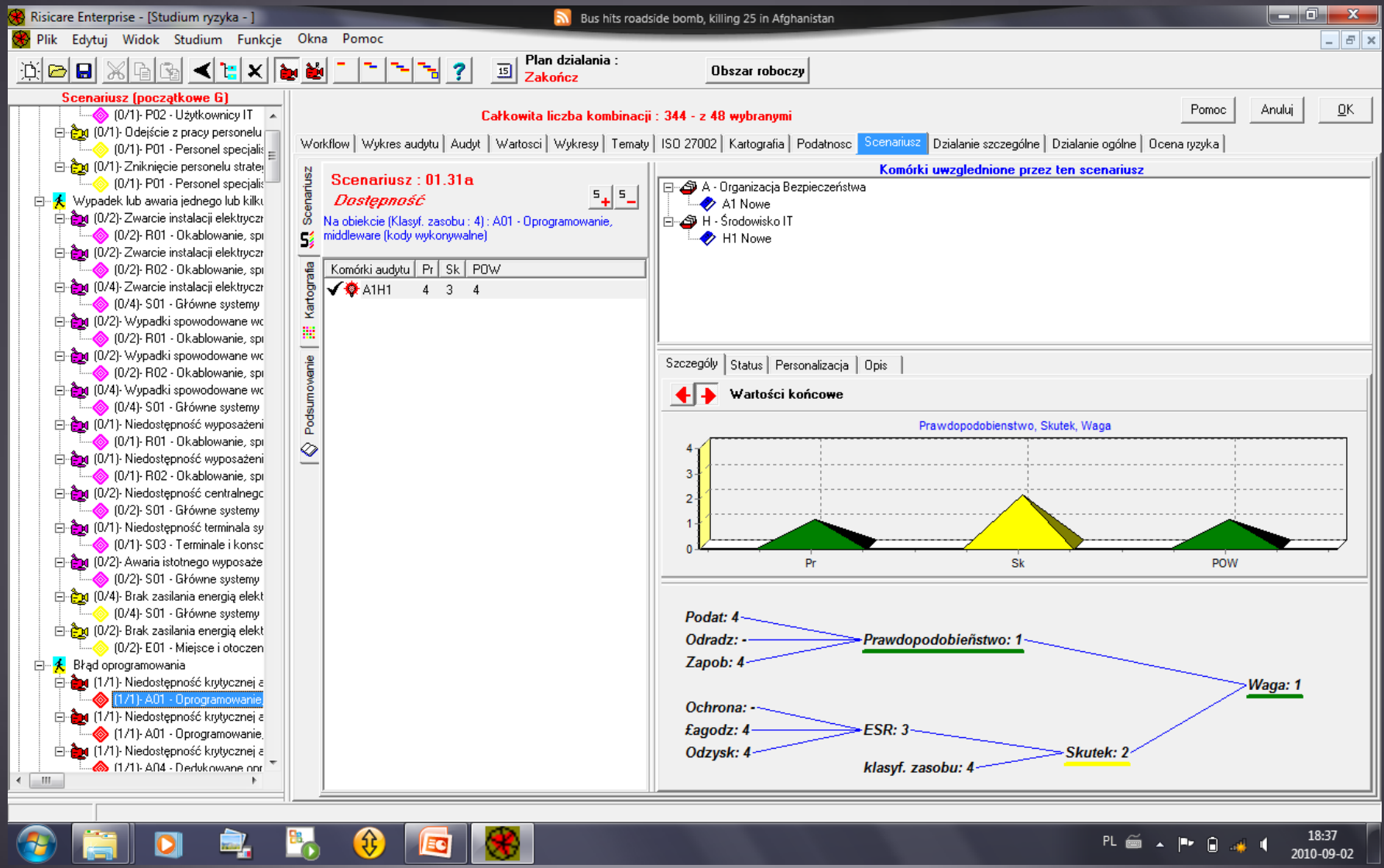
Etapy Analizy Ryzyka w/g. Mehari

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



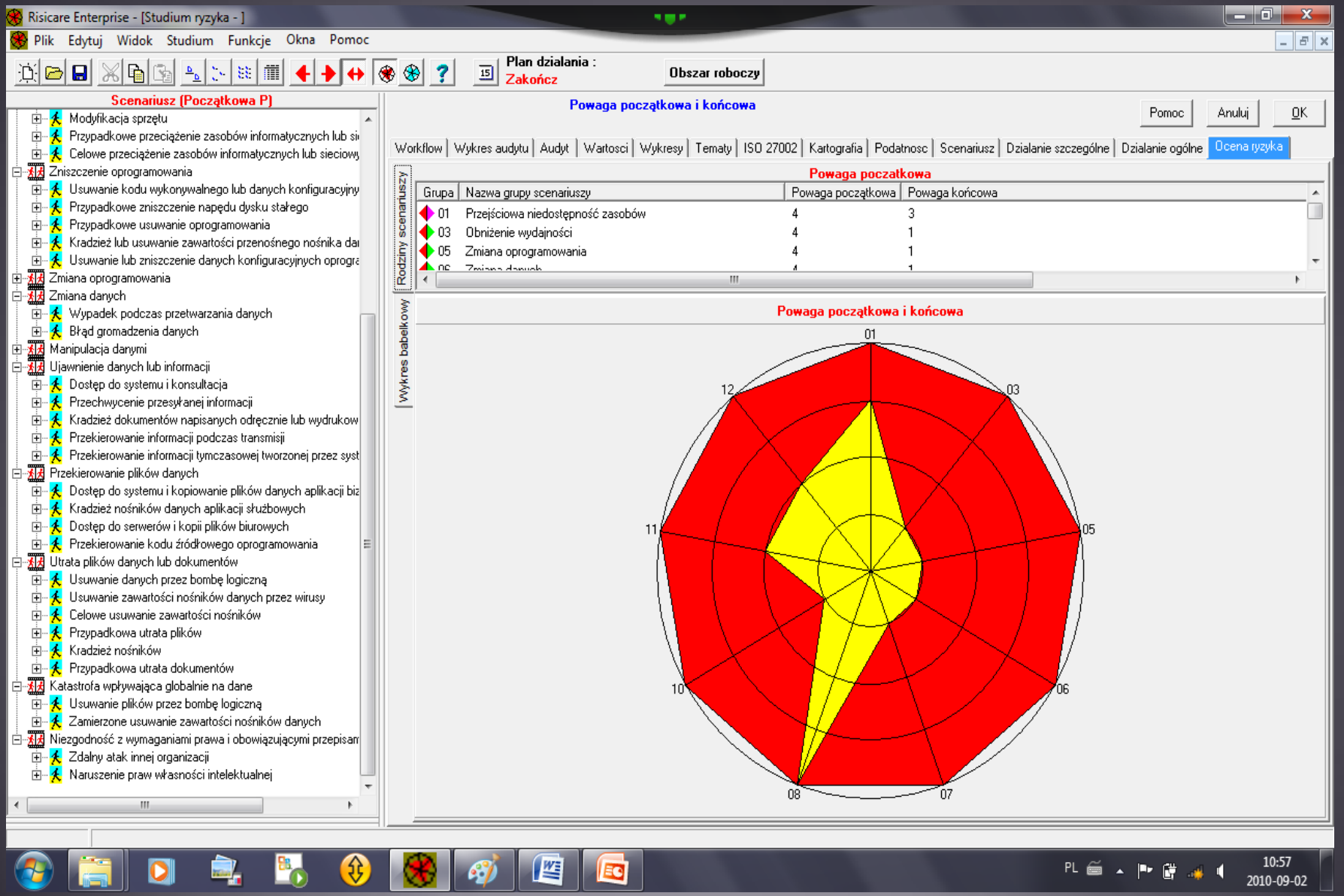
Etapy Analizy Ryzyka w/g. Mehari

Zobrazowanie ryzyka dla każdego ze scenariuszy po wdrożeniu środków zaradczych



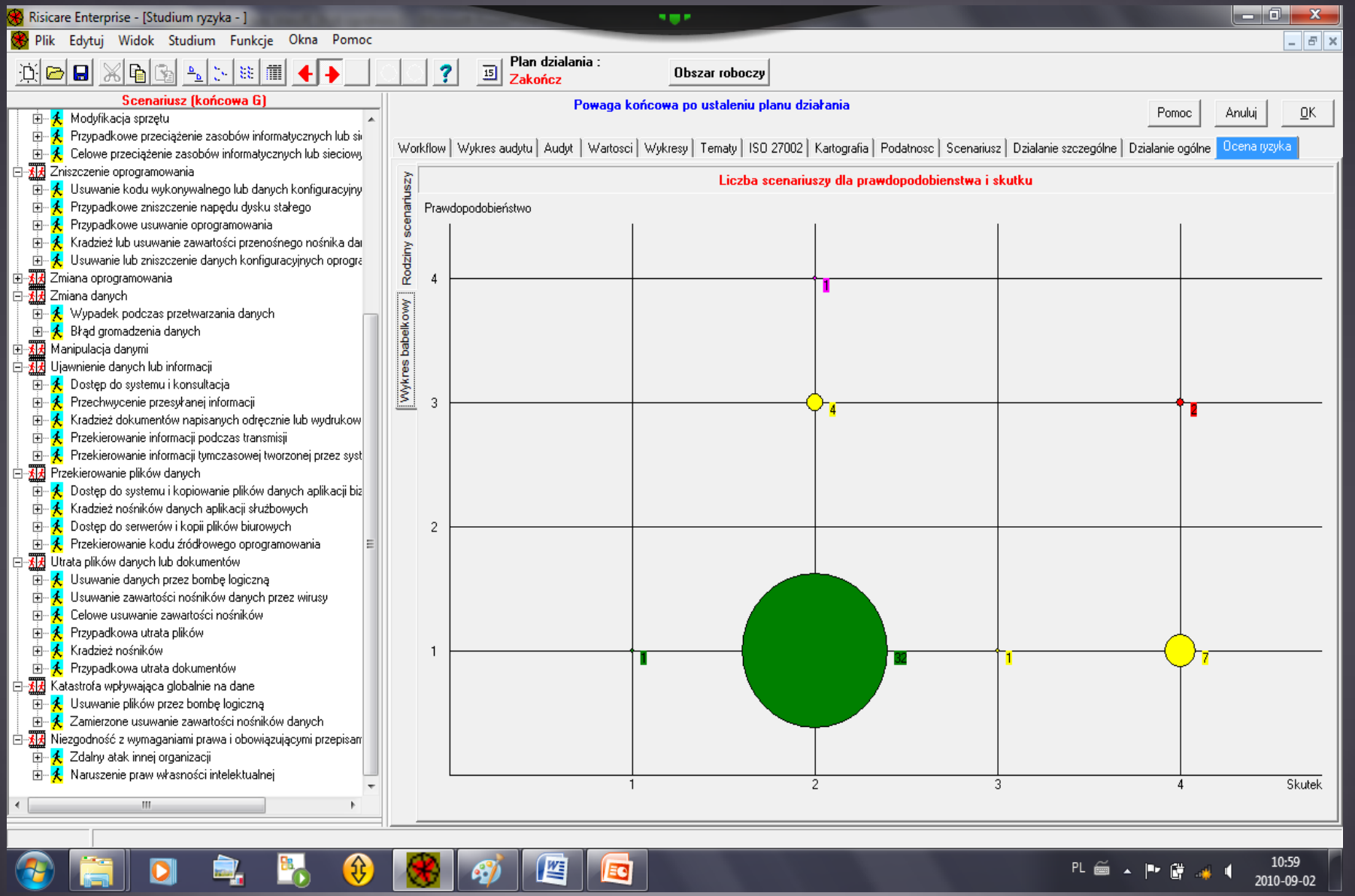
Etapy Analizy Ryzyka w/g. Mehari

Ryzyko systemu po wdrożeniu środków zaradczych



Etapy Analizy Ryzyka w/g. Mehari

Ryzyko systemu po wdrożeniu środków zaradczych



BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH

SZCZECIŃSKI PARK NAUKOWO - TECHNOLOGICZNY

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 oprogramowani,
- metod uwierzytelnienia i autoryzacji w systemach informatycznych.

BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH

SZCZECIŃSKI PARK NAUKOWO - TECHNOLOGICZNY

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 wdrażaniu środków zaradczych (Oprogramowanie Risicare)

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 współudział w tworzeniu polityki i procedur bezpieczeństwa dla systemu informacyjnego.

BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH

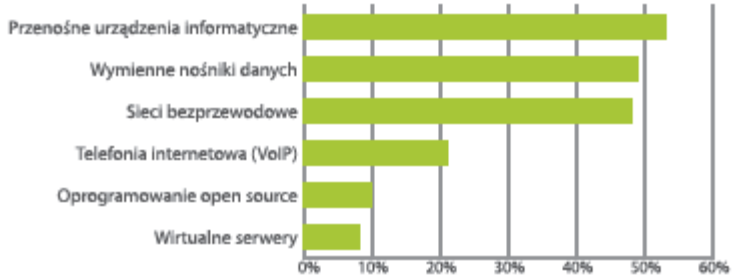
SZCZECIŃSKI PARK NAUKOWO - TECHNOLOGICZNY

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,
- współudział 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

SZCZECIŃSKI PARK NAUKOWO - TECHNOLOGICZNY

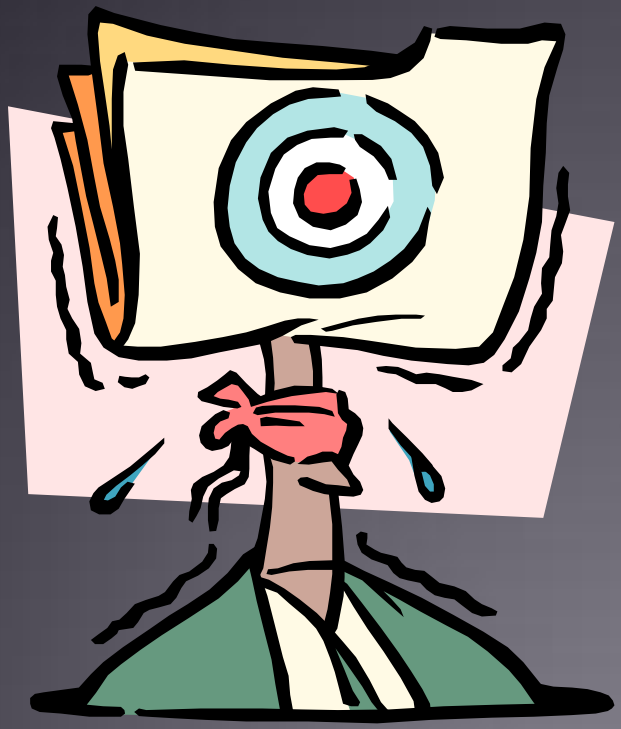
AUDYTY i SZKOLENIA

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?