



# Jak zapewnić bezpieczeństwo firmy – Metodyka SABSA

4 czerwca 2008

---

# Plan prezentacji

---

- ▶ Aspekty bezpieczeństwa organizacji
- ▶ Standardy jako narzędzie zarządzania bezpieczeństwem
- ▶ Model wdrażania i zarządzania mechanizmami bezpieczeństwa
- ▶ Architektura bezpieczeństwa – SABSA
- ▶ Porównanie SABSA z wybranymi standardami
- ▶ Podsumowanie

# Aspekty bezpieczeństwa organizacji

---

- ▶ Standardy i najlepsze praktyki
- ▶ Kultura organizacji – zbiór wypracowanych przez organizację zasad i zachowań. Zmiany zachowania dotyczące kwestii bezpieczeństwa:
  - ▶ ewolucja
  - ▶ rewolucja
- ▶ Otoczenie organizacji:
  - ▶ wymagania prawne i ustawodawcze
  - ▶ kwestie związane z działalnością instytucji kontrolujących
  - ▶ firmy współpracujące / kontrahenci

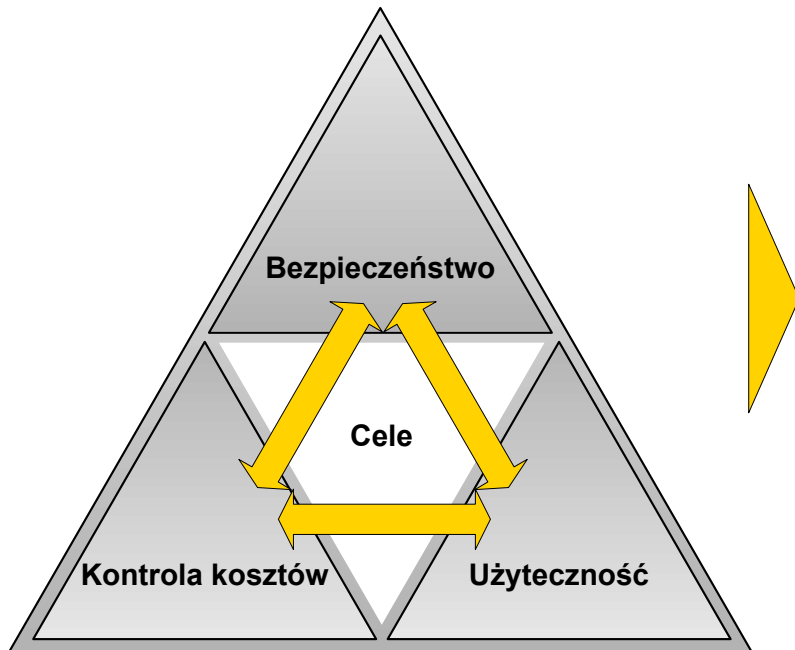
# Standardy jako narzędzie zarządzania bezpieczeństwem

---

- ▶ ISO/IEC 27001 (znana wcześniej jako brytyjska norma BS 7799-2) – specyfikacja systemów zarządzania bezpieczeństwem informacji
- ▶ ISO/IEC 17799 (znana wcześniej jako brytyjska norma BS 7799-1) – praktyczne zasady zarządzania bezpieczeństwem informacji
- ▶ CobiT – niezależny od technologii zbiór zasad kontroli systemów IT
- ▶ Norma ISO/IEC 20000 (jej poprzednikiem był brytyjski standard BS 15000) została zbudowana w oparciu o bibliotekę ITIL, która jest zbiorem dokumentów prezentujących wytyczne dotyczące zarządzania usługami IT – ISO/IEC 20000 ma na celu standaryzację obszaru IT
- ▶ AS 8018 (australijski odpowiednik BS 15000) zakres stosowania normy jest rozszerzony na organizacje sprzedające systemy informatyczne, które chcą zapewnić, że ich produkty są dostosowane do potrzeb klienta i zgodnie z nimi skonfigurowane

# Model wdrażania i zarządzania mechanizmami bezpieczeństwa

Sprzeczne cele wdrażania mechanizmów bezpieczeństwa:



Architektura bezpieczeństwa

- ▶ Zestaw zasad, zaleceń, wzorców i standardów z zakresu bezpieczeństwa wraz z opisem ich wzajemnego powiązania w odniesieniu do uwarunkowań biznesowych
- ▶ Odejście od koncepcji standardowego podejścia analizy poszczególnych obszarów
- ▶ Analiza bezpieczeństwa według łańcucha wartości
- ▶ Analiza bezpieczeństwa z perspektywy poszczególnych procesów biznesowych
- ▶ Ewolucyjne podejście do przeprowadzania zmian

# Architektura bezpieczeństwa – SABSA (1/6)

---

SABSA (Sherwood Applied Business Security Architecture) przedstawia całościowe podejście do zarządzania usługami i architekturą Bezpieczeństwa w przedsiębiorstwie

SABSA jest wykorzystywana przez wiele organizacji na świecie do budowy architektury bezpieczeństwa przedsiębiorstwa i zarządzania usługami

Metodyka SABSA jest zgodna z następującymi standardami:

- ▶ ITIL / ISO 20000
- ▶ ISO 27001 / 17799
- ▶ CobiT
- ▶ BS 15000 / AS 8018

# Architektura bezpieczeństwa – SABSA (2/6)

Całościowe podejście do zarządzania usługami i architekturą bezpieczeństwa w przedsiębiorstwie opiera się na sześciu warstwach\*:

- ▶ **kontekstową**, obejmującą umiejscowienie Bezpieczeństwa i jego roli w Biznesie
- ▶ **konceptyjną**, zawierającą wysokopoziomowy opis Bezpieczeństwa – Strategię Bezpieczeństwa
- ▶ **logiczną**, zawierającą model organizacji, model przepływu informacji i Politykę Bezpieczeństwa
- ▶ **fizyczną**, opisującą procedury, mechanizmy, platformę i infrastrukturę sieciową
- ▶ **komponentową**, obejmującą bezpośrednie narzędzia wdrożenia Bezpieczeństwa – standardy, protokoły, certyfikaty
- ▶ **operacyjną**, warstwę spinającą pozostałe warstwy w codziennym funkcjonowaniu organizacji – Bezpieczeństwo aplikacji, sieci, pomoc techniczna



\* Warstwowy model architektury bezpieczeństwa opracowany został na bazie siatki Zachmana

# Architektura bezpieczeństwa – SABSA (3/6)

---

Rozpatrywane aspekty architektury bezpieczeństwa według metodyki SABSA:

- ▶ Co próbujemy chronić? – aktywa chronione przez architekturę bezpieczeństwa
- ▶ Dlaczego to robimy? – motywacja do podejmowania działań
- ▶ Jak to robimy? – wykonywane działania
- ▶ Kto to wykonuje? – aspekty organizacyjne
- ▶ Gdzie podejmujemy działania? – obszary, w których podejmowane są działania
- ▶ Kiedy podejmujemy działania? – aspekty czasowe podejmowanych działań

Czy odpowiedzi na powyższe pytania byłyby identyczne u prezesa i szeregowego pracownika?

# Architektura bezpieczeństwa – SABSA (4/6)

Proces projektowania architektury bezpieczeństwa polega na rozważeniu aspektów w poszczególnych warstwach macierzy SABSA

	Zasoby (Co ?)	Motywacja (Dlaczego ?)	Proces (Jak ?)	Ludzie (Kto ?)	Miejsce (Gdzie ?)	Czas (Kiedy ?)
Warstwa kontekstowa	Biznes	Model ryzyka biznesowego	Model procesów biznesowych	Organizacja biznesowa i jej powiązania	Geografia biznesu	Zależności czasowe biznesu
Warstwa koncepcyjna	Profil atrybutów biznesowych	Cele kontrolne	Strategia Bezpieczeństwa i warstwy architektury	Model jednostki bezpieczeństwa i struktury zaufania	Model domeny bezpieczeństwa	Czasy życia i terminy związane z bezpieczeństwem
Warstwa logiczna	Model informacyjny biznesu	Polityka Bezpieczeństwa	Usługi bezpieczeństwa	Schemat jednostek i profile uprawnień	Definicje bezpieczeństwa i ich powiązania	Cykl procesów bezpieczeństwa
Warstwa fizyczna	Model danych biznesu	Reguły bezpieczeństwa, praktyki i procedury	Mechanizmy bezpieczeństwa	Użytkownicy, aplikacje i interfejs użytkownika	Platforma i infrastruktura sieci	Czas wykonanie struktury kontrolnej
Warstwa komponentowa	Szczegółowe struktury danych	Standardy bezpieczeństwa	Produkty i narzędzia bezpieczeństwa	Tożsamości, funkcje, czynności i ACL	Procesy, węzły, adresy i protokoły	Kolejkowanie kroków bezpieczeństwa
Warstwa operacyjna	Zapewnienie ciągłości operacyjnej	Zarządzanie ryzykiem operacyjnym	Zarządzanie i wsparcie usługami bezpieczeństwa	Zarządzanie i wsparcie użytkowników i aplikacji	Bezpieczeństwo systemów, sieci i platform	Rozkład czynności bezpieczeństwa

# Architektura bezpieczeństwa – SABSA (5/6)

Na etapie projektowania architektury bezpieczeństwa powinniśmy uwzględnić zasady zarządzania modelem i mechanizmami bezpieczeństwa w organizacji

	Zasoby (Co ?)	Motywacja (Dlaczego ?)	Proces (Jak ?)	Ludzie (Kto ?)	Miejsce (Gdzie ?)	Czas (Kiedy ?)
Warstwa kontekstowa	Analiza procesów biznesowych, Klasyfikacja informacji	Tworzenie strategii Bezpieczeństwa, Analiza ryzyk biznesowych	Program zarządzania Bezpieczeństwem Informacji	Zarządzanie organizacją Bezpieczeństwa	Zarządzanie segmentami działalności biznesowej	Zarządzanie harmonogramem biznesowym
Warstwa koncepcyjna	Zarządzanie ciągłością działania	Audyt Bezpieczeństwa, Mierniki, Benchmarking	Reakcja na Incydent, Planowanie awaryjne, Program kontroli zmiany	Trening, Budowanie świadomości	Zarządzanie domeną Bezpieczeństwa	Zarządzanie harmonogramem operacji Bezpieczeństwa
Warstwa logiczna	Bezpieczeństwo Informacji, Integralność Systemu	Tworzenie strategii bezpieczeństwa, Zgodność strategii, Monitorowanie	Monitorowanie zdarzeń, Rozwój procesów, Zarządzanie usługami Bezpieczeństwa, Mierniki rozwoju systemu, Zarządzanie Konfiguracją	Kontrola dostępu, Zarządzanie profilami	Administracja i zarządzanie Bezpieczeństwem aplikacji	Zarządzanie terminami dla aplikacji (deadlines)
Warstwa fizyczna	Bezpieczeństwo Baz Danych, Integralność oprogramowania	Analiza podatności na ryzyko, Testy penetracyjne, Ocena zagrożeń	Definicja reguł, Zarządzanie krytyczne, Utrzymanie ACL, Zarządzanie kopiami zapasowymi, logami, oprogramowaniem antywirusowym, informatyka śledcza	Wsparcie użytkownika i Help Desk	Zarządzanie Bezpieczeństwem Sieci, Zarządzanie Bezpieczeństwem lokalizacji	Starzenie się kont użytkowników, Administrowanie oknami czasowymi w kontroli dostępu
Warstwa komponentowa	Bezpieczeństwo i spójność Produktów i Narzędzi	Powiadomienie CERT, Badanie zagrożeń i słabych punktów	Dostarczanie produktów, Zarządzanie projektem, Zarządzanie operacjami	Zarządzanie personelem, Administrowanie użytkownikami	Platforma, Zarządzanie Bezpieczeństwem wyposażenia i miejsc pracy	Konfiguracja czasu przerwy, Szczegółowa sekwencja działań

# Architektura bezpieczeństwa – SABSA (6/6)

Możliwe uzasadnienie inwestycji w bezpieczeństwo oraz rozliczanie się z podjętych działań:





# Porównanie SABSA ze standardami (1/2)

## SABSA vs. CobiT i ISO 17799

Powiązania pomiędzy CobiT i ISO 17799 a poszczególnymi aspektami warstw macierzy SABSA

	Zasoby (Co ?)	Motywacja (Dlaczego ?)	Proces (Jak ?)	Ludzie (Kto ?)	Miejsce (Gdzie ?)	Czas (Kiedy ?)
Warstwa kontekstowa	Biznes	Model ryzyka biznesowego	Model procesów biznesowych	Organizacja biznesowa i jej powiązania	Geografia biznesu	Zależności czasowe biznesu
Warstwa koncepcyjna	Profil atrybutów biznesowych	Cele kontrolne	Strategia Bezpieczeństwa i warstwy architektury	Model jednostki bezpieczeństwa i struktury zaufania	Model domeny bezpieczeństwa	Czasy życia i terminy związane z bezpieczeństwem
Warstwa logiczna	Model informacyjny biznesu	Polityka Bezpieczeństwa	Usługi bezpieczeństwa	Schemat jednostek i profile uprawnień	Definicje bezpieczeństwa i ich powiązania	Cykl procesów bezpieczeństwa
Warstwa fizyczna	Model danych biznesu	Reguły bezpieczeństwa, praktyki i procedury	Mechanizmy bezpieczeństwa	Użytkownicy, aplikacje i interfejs użytkownika	Platforma i infrastruktura sieci	Czas wykonanie struktury kontrolnej
Warstwa komponentowa	Szczegółowe struktury danych	Standardy bezpieczeństwa	Produkty i narzędzia bezpieczeństwa	Tożsamości, funkcje, czynności i ACL	Procesy, węzły, adresy i protokoły	Kolejkowanie kroków bezpieczeństwa


-  Elementy opisane w CobiT
-  Elementy opisane w ISO 17799

# Porównanie SABSA ze standardami (2/2)

## SABSA vs. ITIL

Powiązania pomiędzy ITIL a poszczególnymi aspektami warstw macierzy SABSA w ujęciu operacyjnym

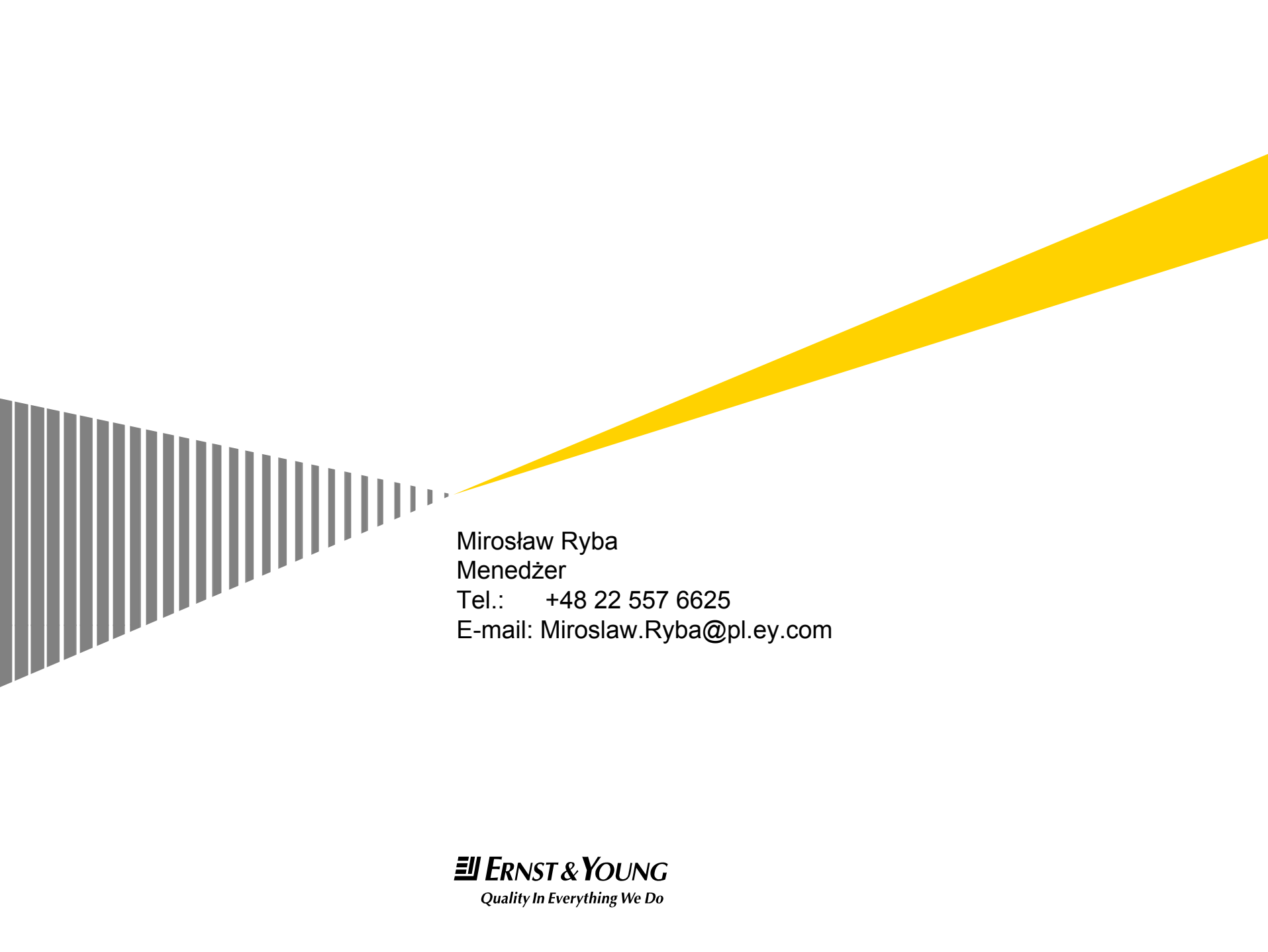
	Zasoby (Co ?)	Motywacja (Dlaczego ?)	Proces (Jak ?)	Ludzie (Kto ?)	Miejsce (Gdzie ?)	Czas (Kiedy ?)
Warstwa kontekstowa	Analiza procesów biznesowych, Klasyfikacja informacji	Tworzenie strategii Bezpieczeństwa, Analiza ryzyk biznesowych	Program zarządzania Bezpieczeństwem Informacji	Zarządzanie organizacją Bezpieczeństwa	Zarządzanie segmentami działalności biznesowej	Zarządzanie harmonogramem biznesowym
Warstwa koncepcyjna	Zarządzanie ciągłością działania	Audyty Bezpieczeństwa, Mierniki, Benchmarking	Reakcja na Incydent, Planowanie awaryjne, Program kontroli zmiany	Trening, Budowanie świadomości	Zarządzanie domeną Bezpieczeństwa	Zarządzanie harmonogramem operacji Bezpieczeństwa
Warstwa logiczna	Bezpieczeństwo Informacji, Integralność Systemu	Tworzenie strategii bezpieczeństwa, Zgodność strategii, Monitorowanie	Monitorowanie zdarzeń, Rozwój procesów, Zarządzanie usługami Bezpieczeństwa, Miarość zasobów systemu, Zarządzanie Konfiguracją	Kontrola dostępu, Zarządzanie profilami	Administracja i zarządzanie Bezpieczeństwem aplikacji	Zarządzanie terminami dla aplikacji (deadlines)
Warstwa fizyczna	Bezpieczeństwo Baz Danych, Integralność oprogramowania	Analiza podatności na ryzyko, Testy penetracyjne, Ocena zagrożeń	Definicja reguł, Zarządzanie krytyczne, Utrzymanie ACL, Zarządzanie kopiami zapasowymi, logami, oprogramowaniem antywirusowym, informatyka śledcza	Wsparcie użytkownika i Help Desk	Zarządzanie Bezpieczeństwem Sieci, Zarządzanie Bezpieczeństwem lokalizacji	Starzenie się kont użytkowników, Administrowanie oknami czasowymi w kontroli dostępu
Warstwa komponentowa	Bezpieczeństwo i spójność Produktów i Narzędzi	Powiadomienie CERT, Badanie zagrożeń i słabych punktów	Dostarczanie produktów, Zarządzanie projektem, Zarządzanie operacjami	Zarządzanie personelem, Administrowanie użytkownikami	Platforma, Zarządzanie Bezpieczeństwem wyposażenia i miejsc pracy	Konfiguracja czasu przerwy, Szczegółowa sekwencja działań

 Elementy opisane w ITIL

# Podsumowanie

---

- ▶ SABSA to kompleksowa metodyka zarządzania bezpieczeństwem organizacji
- ▶ SABSA jest zgodna z wykorzystywanymi obecnie standardami w obszarze bezpieczeństwa
- ▶ Standardy definiują co powinno być wdrożone, natomiast SABSA wskazuje jak tego dokonać w danych uwarunkowaniach biznesowych
- ▶ SABSA ułatwia dialog pomiędzy organizacją Bezpieczeństwa a przedstawicielami Biznesu
- ▶ SABSA jest stosowana w wielu organizacjach komercyjnych i rządowych
- ▶ SABSA została wykorzystana przez Ministerstwo Obrony Narodowej Wielkiej Brytanii do stworzenia Architektury Zapewnienia Informacji Bezpieczeństwa



Mirosław Ryba  
Menedżer  
Tel.: +48 22 557 6625  
E-mail: [Miroslaw.Ryba@pl.ey.com](mailto:Miroslaw.Ryba@pl.ey.com)