

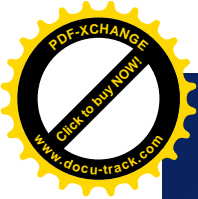


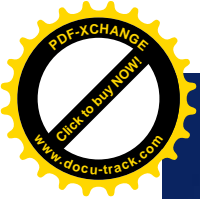
URZĄD KOMISJI NADZORU FINANSOWEGO

Zarządzanie

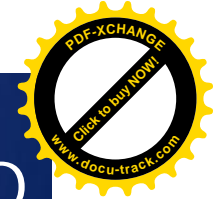
bezpieczeństwem informacji

dr inż. Janusz Zawiła-Niedźwiecki





URZĄD KOMISJI NADZORU FINANSOWEGO



Plan prezentacji

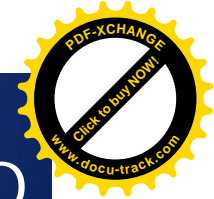
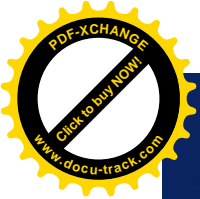
§ **Bezpieczeństwo informacji**

§ **Wymogi prawne**

§ **Źródła dobrych praktyk**

§ **Teraźniejszość - norma PN-ISO/IEC-17799**

§ **Przyszłość – rodzina norm ISO-27000**

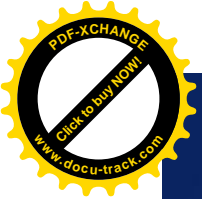


Bezpieczeństwo informacji

oznacza zachowanie:

- Poufności : zapewnienie dostępu do informacji tylko osobom upoważnionym
- Integralności: zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania
- Dostępności: zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne

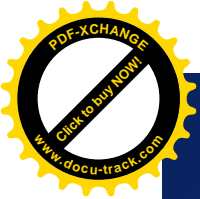
niezaprzeczalność, rozliczalność, jednoznaczność, niezawodność, bezpieczeństwo



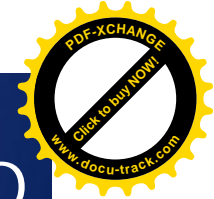
URZĄD KOMISJI NADZORU FINANSOWEGO

Prawne wymogi ochrony informacji

- **Kodeksy: cywilny, karny, pracy**
- **Ustawa o ochronie danych osobowych**
- **Ustawa o ochronie informacji niejawnych**
- **Ustawa o zwalczaniu nieuczciwej konkurencji**
- **Ustawa o ochronie osób i mienia**
- **Ustawa o rachunkowości**
- **Ustawa o prawie autorskim i prawach pokrewn.**
- **Ustawa o dostępie do informacji publicznej**
- **Ustawa o ochronie baz danych**
- **Ustawa o świadczeniu usług drogą elektroniczną**



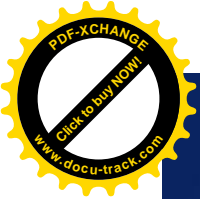
URZĄD KOMISJI NADZORU FINANSOWEGO



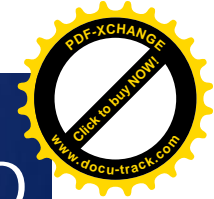
Art. 11 ust. 4

Ustawy o zwalczaniu nieuczciwej konkurencji

Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.



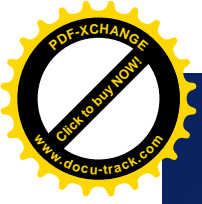
URZĄD KOMISJI NADZORU FINANSOWEGO



Art. 100 Kodeksu pracy

**§ 2. Pracownik jest obowiązany
w szczególności:**

**4) dbać o dobro zakładu pracy, chronić jego
mienie oraz zachować w tajemnicy informacje,
których ujawnienie mogłoby narazić
pracodawcę na szkodę,**

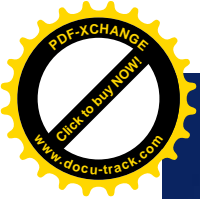


URZĄD KOMISJI NADZORU FINANSOWEGO

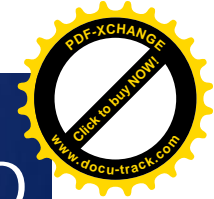
Art. 6. 1. Ustawy o ochronie danych osobowych

W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej

- Ochrona zbiorów danych osobowych:
 - Klientów
 - Pracowników:
 - kadrowe
 - służbowe
 - powierzonych do przetwarzania.

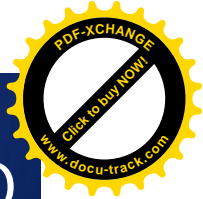
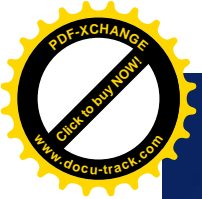


URZĄD KOMISJI NADZORU FINANSOWEGO



Tajemnice zawodowe

- bankowa
- handlowa
- ubezpieczeniowa
- maklerska
- statystyczna
- wynalazcza
- lekarska
- skarbowa
- usług certyfikacyjnych



Odpowiedzialność karna za naruszenie zasad ochrony informacji

- **Przepisy Kodeksu Karnego dotyczące przestępstw przeciwko ochronie informacji**
- **Przepisy karne Ustawy o zwalczaniu nieuczciwej konkurencji**
- **Przepisy karne Kodeksu pracy**
- **Przepisy karne Ustawy o ochronie danych osobowych**
- **Przepisy karne chroniące tajemnice zawodowe**



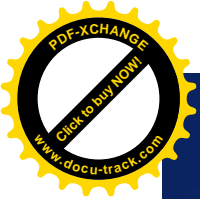
URZĄD KOMISJI NADZORU FINANSOWEGO

Źródła dobrych praktyk

§ normy polskie i międzynarodowe

§ metody projektowania rozwiązań

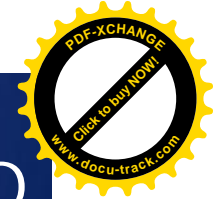
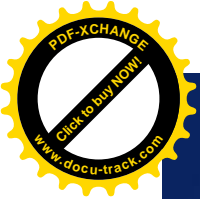
§ rekomendacje branżowe



URZĄD KOMISJI NADZORU FINANSOWEGO

Źródła dobrych praktyk

- **PN-I-133555-1:1999 Pojęcia i modele bezpieczeństwa systemów informatycznych**
- **ISO/IEC TR 13335-3:1998 Techniki zarządzania bezpieczeństwem systemów informatycznych**
- **ISO/IEC TR 13335-4:2000 Dobór zabezpieczeń**
- **ISO/IEC TR 13335-5:2001 Zabezpieczenia połączeń zewnętrznych**
- **PN-ISO/IEC 15408-1:2002 Kryteria oceny zabezpieczeń. Model ogólny**
- **PN-ISO/IEC 15408-2:2005 Wymagania bezpieczeństwa funkcjonalnego**



Źródła dobrych praktyk

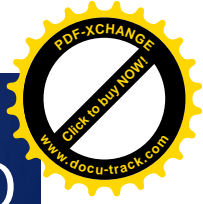
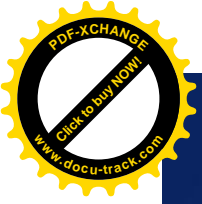
- **PN-ISO/IEC 15408-3:2005 Wymagania uzasadnienia zaufania do zabezpieczeń**
- **PN-ISO/IEC 17799:2003 Praktyczne zasady zarządzania bezpieczeństwem informacji**
- **PN-ISO-27001:2006 Wytyczne do stosowania**
- **BS 15000-1:2002 Procesy zarządzania usługami informatycznymi**
- **BS 15000-2:2003 Praktyczne zasady zarządzania usługami informatycznymi**



URZĄD KOMISJI NADZORU FINANSOWEGO

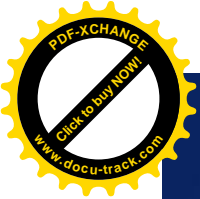
Źródła dobrych praktyk

- metoda COBIT – www.isaca.org.pl
- metoda ITIL - www.iti-itsm-world.com
- metoda TISM – www.ensi.net

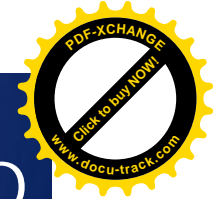


Źródła dobrych praktyk

- **Rekomendacja D GINB Zarządzanie ryzykami towarzyszącymi systemom informatycznym**
- **Rekomendacja M GINB Zarządzanie ryzykiem operacyjnym (wg rekomendacji Komitetu Bazylejskiego)**



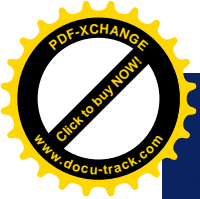
URZĄD KOMISJI NADZORU FINANSOWEGO



Teraźniejszość – norma PN-ISO/IEC-17799:2003*

- Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji
Zalecenia dotyczące zarządzania bezpieczeństwem informacji
- Podstawa dla rozwijania wewnętrznych standardów bezpieczeństwa
- Uzupełnienie odpowiednich regulacji i przepisów prawnych dotyczących ochrony informacji

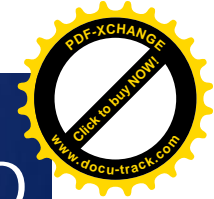
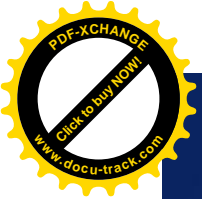
* The Polish FSA, 2007
wersja ISO jest już z 2005



URZĄD KOMISJI NADZORU FINANSOWEGO

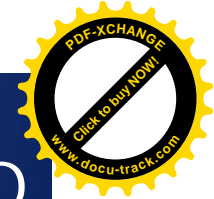
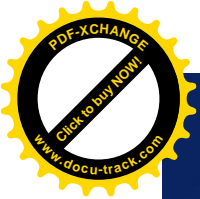
Zakres tematyczny normy

- Dokument Polityki Bezpieczeństwa
- Organizacja bezpieczeństwa
- Klasyfikacja i kontrola aktywów
- Bezpieczeństwo osobowe
- Bezpieczeństwo fizyczne i środowiskowe
- Kontrola dostępu do systemu
- Rozwój i utrzymanie systemu
- Zarządzanie ciągłością działania
- Zgodność z wymogami prawa



Przyszłość – rodzina norm ISO-27000

- ISO 27000 - terminologia
- ISO 27001- specyfikacja systemów zarządzania bezpieczeństwem informacji
- ISO 27002 -zasady zarządzania bezpieczeństwem informacji (ob. PN-ISO/IEC-17799)
- ISO 27003 – wdrażanie ISO 27000 w organizacji
- ISO 27004 - pomiar efektywności zarz. bezp. inf.
- ISO 27005 – zarządzanie ryzykiem bezpiecz. inf.



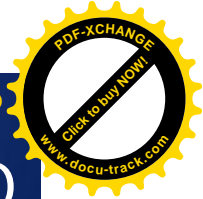
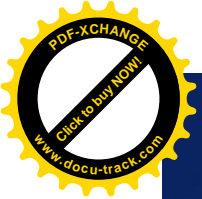
Istota zarządzania bezpieczeństwem inf.

- **Struktura organizacyjna (forum kierownicze, odpowiedzialni za wyznaczanie zasad ochrony, administratorzy stosowania tych zasad, audyt wewnętrzny)**
- **Metoda projektowania i rozwijania rozwiązań**
- **Uświadomienie i analiza ryzyka**
- **Zasady ochrony**

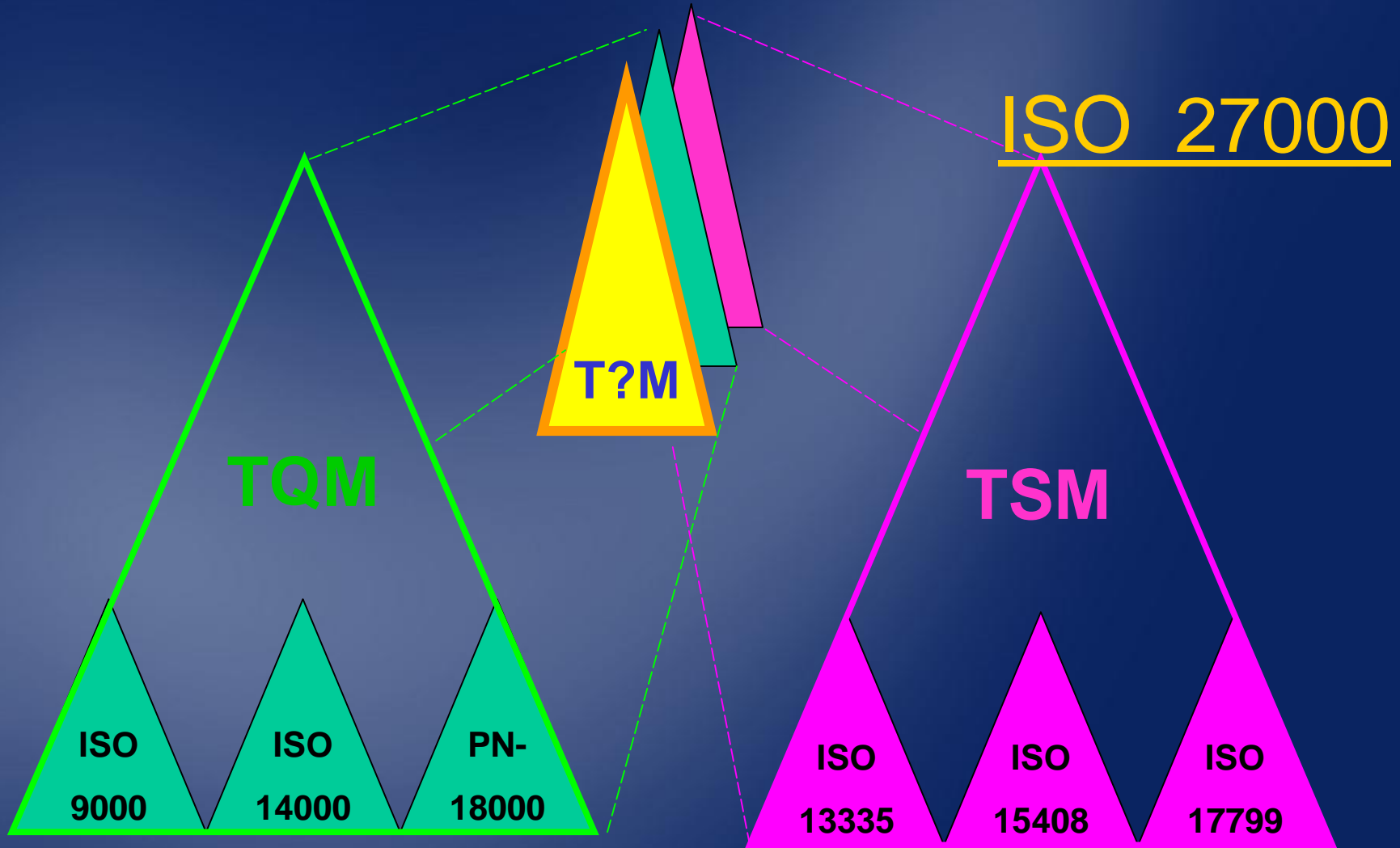


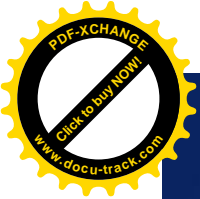
Podejście jakościowe

- analiza procesowa
- stałe doskonalenie (cykl Deminga) wg zasady PDCA (*plan, do, control, act*)



URZĄD KOMISJI NADZORU FINANSOWEGO





URZĄD KOMISJI NADZORU FINANSOWEGO

Stopnie dojrzałości zarządzania bezpieczeństwem informacji *

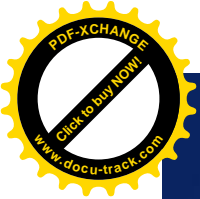
Stopień 0

**-brak zdefiniowania wymagań
bezpieczeństwa**

**Brak
świadomości**

**- bezpieczeństwo traktowane jako
problem poszczególnych
użytkowników**

* wg ISACA

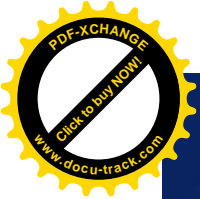


URZĄD KOMISJI NADZORU FINANSOWEGO

Stopnie dojrzałości zarządzania bezpieczeństwem informacji

Stopień I
Początkowy

- świadomość potrzeby
- kierownictwo uważa to za problem IT (typu: prawa dostępu, ochrona antywirusowa)



URZĄD KOMISJI NADZORU FINANSOWEGO

Stopnie dojrzałości zarządzania bezpieczeństwem informacji

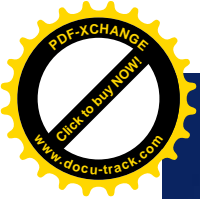
Stopień II

Intuicyjny

- próby tworzenia zabezpieczeń

- brak jednolitego podejścia

- efekty zależne od zaangażowania osób zainteresowanych



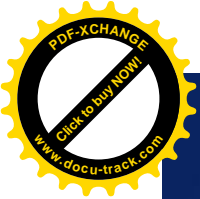
URZĄD KOMISJI NADZORU FINANSOWEGO

Stopnie dojrzałości zarządzania bezpieczeństwem informacji

Stopień III

Zdefiniowany

- zdefiniowane zasady (w tym **Polityka bezpieczeństwa) w całej organizacji**
- procedury bezpieczeństwa są **utrzymywane i komunikowane**
- **brak kontroli stosowania**

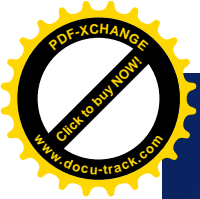


URZĄD KOMISJI NADZORU FINANSOWEGO

Stopnie dojrzałości zarządzania bezpieczeństwem informacji

Stopień IV
Zarządzany

- jednolite podejście dla wszystkich komórek i wszystkich rozwiązań
- obowiązuje perspektywa biznesu
- funkcjonuje mechanizm kontroli stosowania



URZĄD KOMISJI NADZORU FINANSOWEGO

Stopnie dojrzałości zarządzania bezpieczeństwem informacji

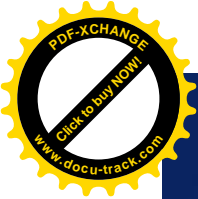
Stopień V

**Optymalizo
wany**

-świadome zarządzanie ryzykiem

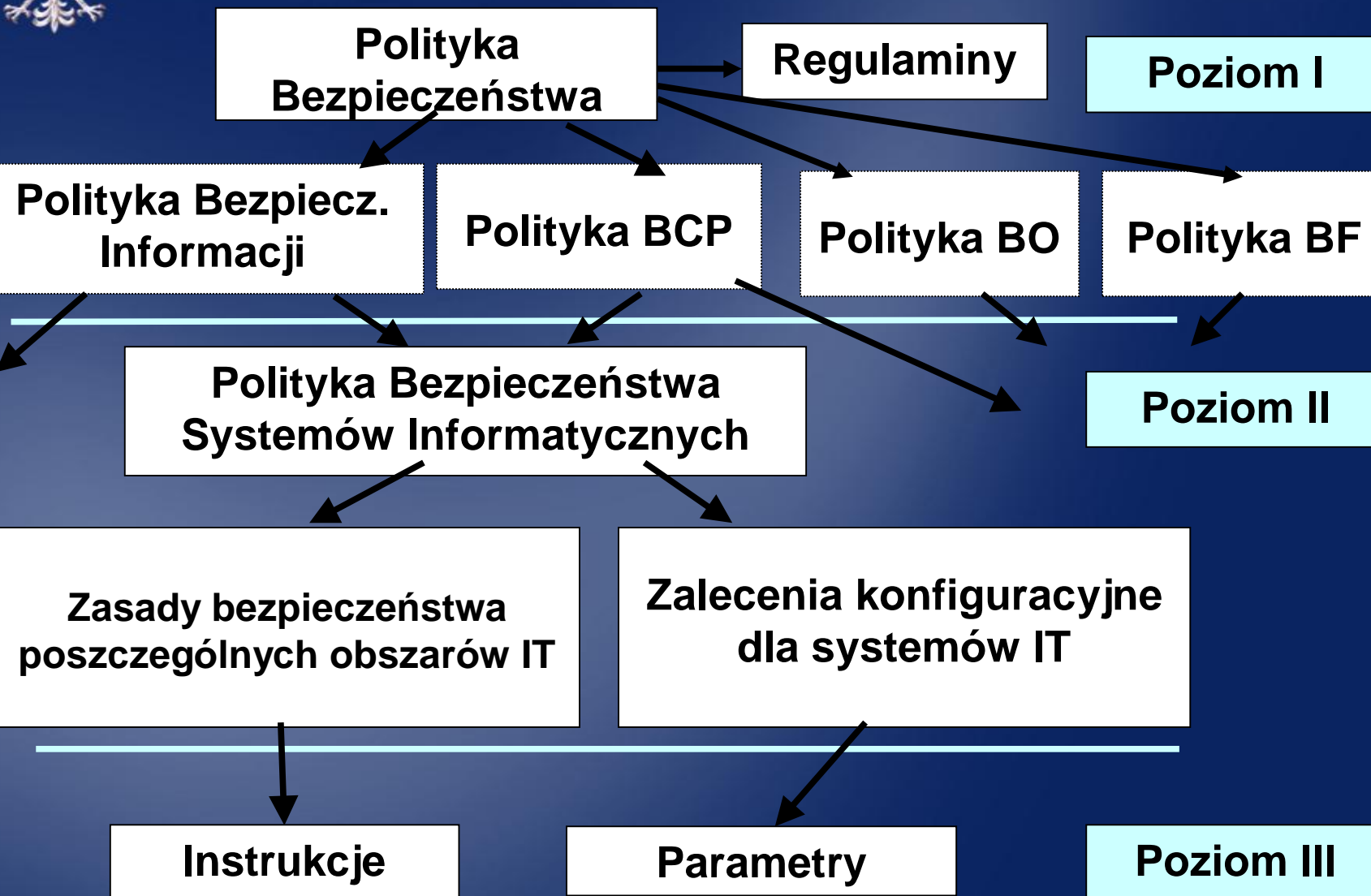
**-zgodność strategii bezpieczeństwa
ze strategią biznesową**

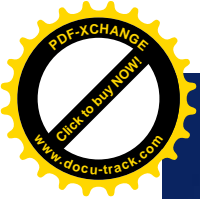
**- zapewnianie bezpieczeństwa jako
proces (wiedza, doskonalenie)**



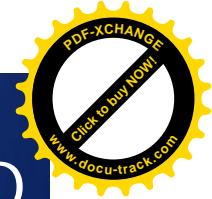
URZĄD KOMISJI NADZORU FINANSOWEGO

Model struktury dokumentów PB





URZĄD KOMISJI NADZORU FINANSOWEGO



Pl. Powstańców Warszawy 1
00-950 Warszawa

tel. + 48 (0 22) 33 26 600

fax. + 48 (0 22) 33 26 602

knf@knf.gov.pl

<http://www.knf.gov.pl>