Trust-IT we wspomaganiu standaryzacji - podejście NOR-STA

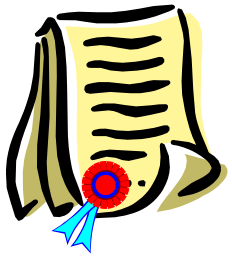
I Spotkanie Komitetu Konsultacyjnego Projektu (KKP)

Katedra Inżynierii Oprogramowania
Politechnika Gdańska

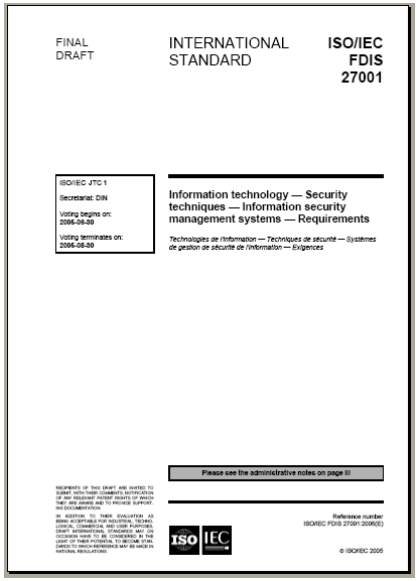
Gdańsk, 31.05-1.06.2010

Charakterystyka podejścia NOR-STA

- Wykorzystanie metodyki Trust-IT (oraz narzędzia TCT) w dziedzinie standaryzacji
- Trust case jako argument za zgodnością czegoś (organizacji, produktu, ...) z normą/standardem
- Podstawowe elementy podejścia:
  - Szablon zgodności
  - Dowód zgodności
  - Ocena zgodności



Szablon zgodności


FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 27001

ISO/IEC JTC 1

Secretariat: DIN

Voting begins on: 2006-06-20

Voting terminates on: 2006-08-20

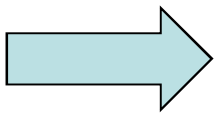
Information technology — Security techniques — Information security management systems — Requirements

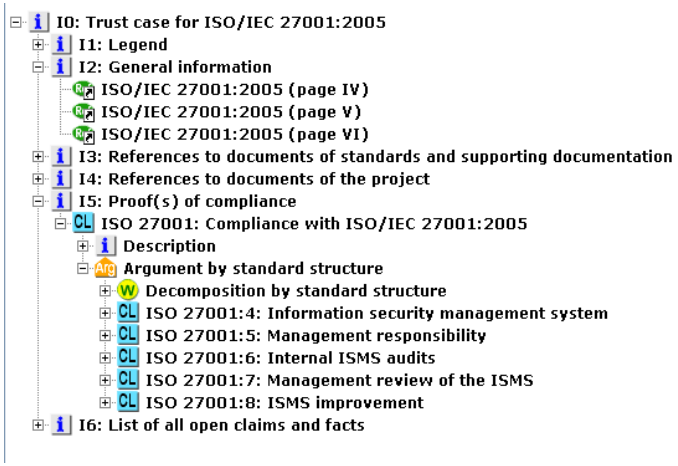
Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Please see the administrative notes on page iii

Reference number ISO/IEC FDIS 27001:2005(E)

© ISO/IEC 2005





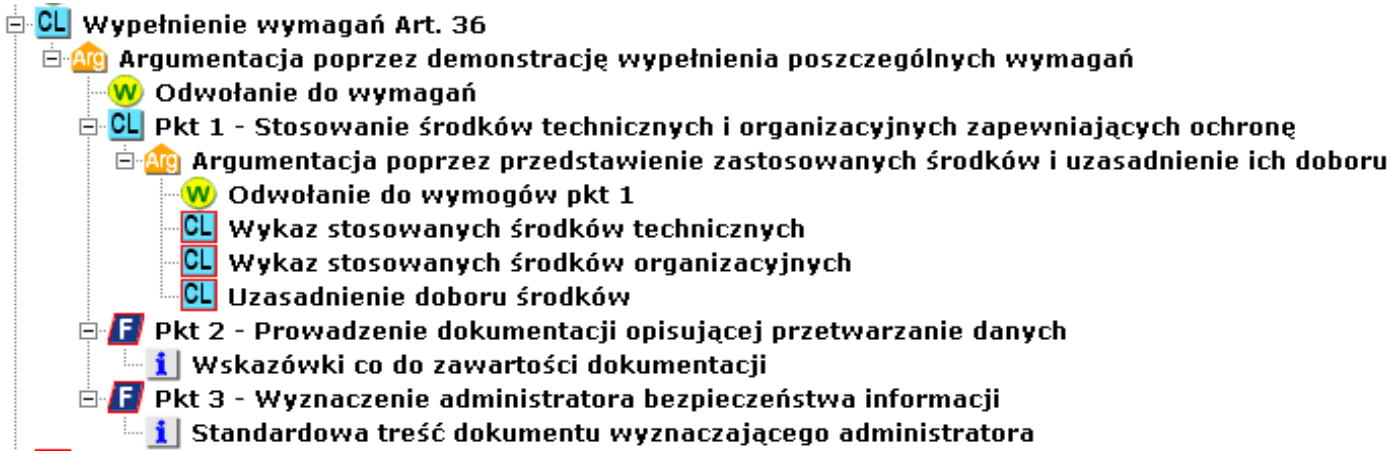
- Odwzorowanie standardu w postaci Trust Case
  - standardy ustrukturalizowane (np. ISO/IEC 27001)
  - standardy nieustrukturalizowane (np. podręcznik promocji PO IG)
- Interpretacja!
- Dodatkowe elementy dzięki możliwościom reprezentacji (np. wewnętrzne zależności między wymaganiami standardu)

Szablon zgodności - przykład

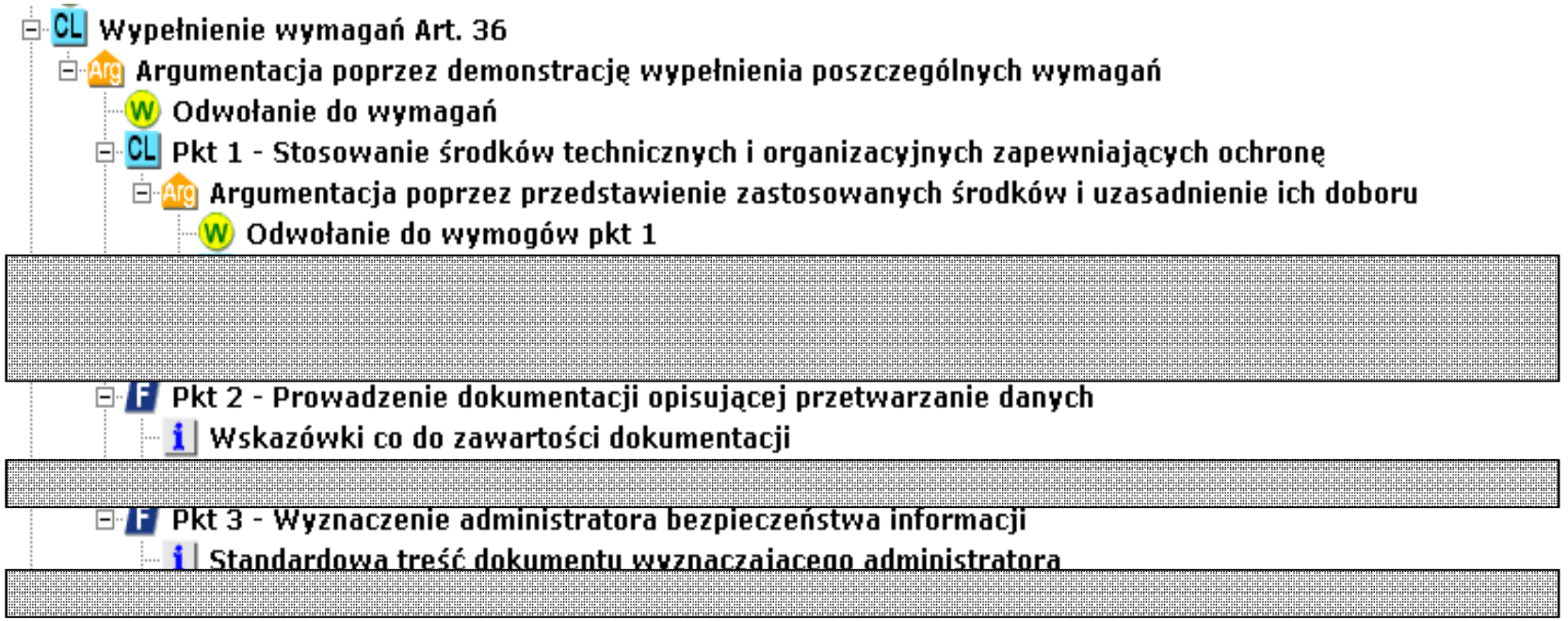
Ustawa o ochronie danych osobowych

Art. 36

1. **Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.**
2. **Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.**
3. **Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.**

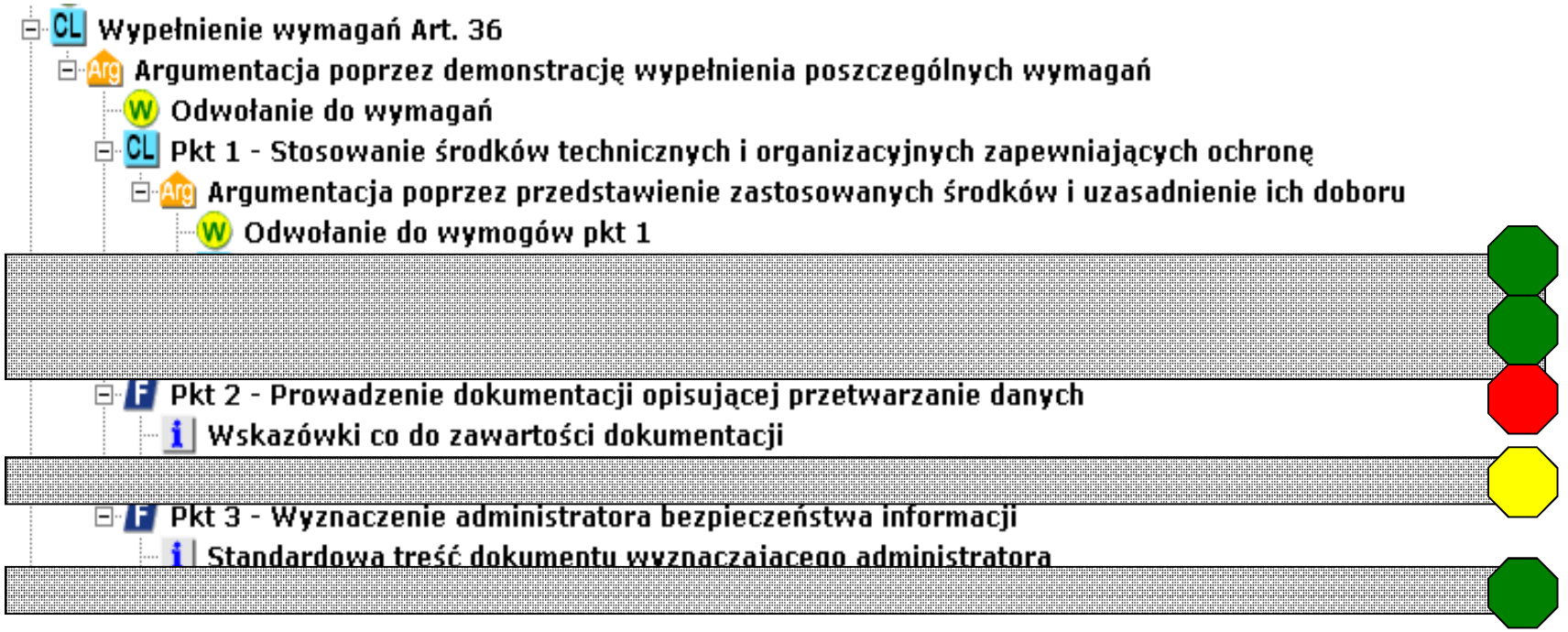


Dowód zgodności



- Uzupełnienie szablonu materiałem dowodowym i szczegółową argumentacją dla konkretnego podmiotu
- Odwołania do różnych zasobów, potencjalnie rozproszonych

Ocena zgodności



- Ocena dokonywana przez eksperta
- Koncentruje się na materiale dowodowym i argumentacji dowodu zgodności, nie szablonu
- Poza ogólnym wynikiem, wskazywane są miejsca gdzie konieczne jest wzmocnienie dowodu zgodności