Tivoli Day 2009

IBM

15.10.2009 r. - Warszawa

TIVOLI DAY 2009

Co nowego w Tivoli Security?

“Nigdy nie lataj samolotami projektowanymi przez optymistów.”

Myślenie poprzez bezpieczeństwo

- Myślenie “negatywowe”
  - “Normalny” architekt: Jak to będzie działać?
  - Architekt bezpieczeństwa: Jak to będzie się psuć?
- Nie istnieje pełne bezpieczeństwo
  - Zwyczajowo: Czy to jest bezpieczne?
  - Słuszniej: Czy to jest wystarczająco bezpieczne?
- Nieustająca czujność
  - Strzelanie do ruchomego celu

Kilka faktów

Co mamy do chronienia w firmie?

Środki/Aktywa (PACS)

Dane (IT Security)

Co wymuszają na nas regulatory?

- Zrozumienie co dzieje się w organizacji
  - Jakie są ryzyka?
    - Co może się stać z moimi krytycznymi elementami biznesu?
  - Jakie incydenty związane są z moim IT?
    - Jak wiele ich jest?
    - Które są „akceptowalne” a które nie?
  - Jaki wpływ może mieć incydent na organizację?
- O co zapyta się audytor?
  - Udowodnij, że wiesz co się dzieje
  - Udowodnij, że twoje krytyczne dane są chronione
  - Udowodnij, że dostęp do krytycznych danych jest kontrolowany

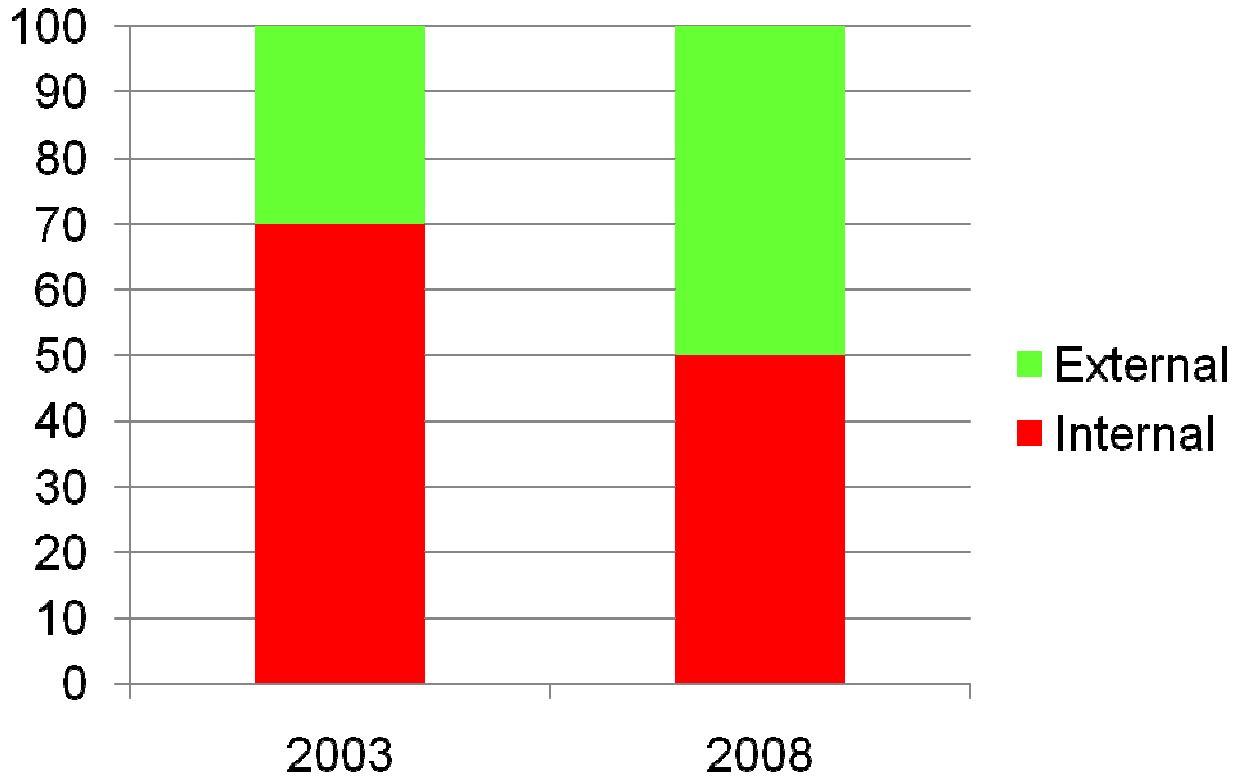
Regulatory

	Prescriptive	Not Prescriptive
Stick	PCI / HIPAA	Sarbanes-Oxley, FISMA, HIPAA, Great majority of domestic regulations
Carrot	[NOTHING]	Basel II

Bezpieczeństwo zawsze jest z czymś w niezgodzie

- Zarządzanie ryzykiem vs Unikanie ryzyka
  - Co możemy zrobić aby 9/11 nie powtórzyło się więcej?
    - Uziemić wszystkie samoloty
  - Kiedy uznamy że jesteśmy bezpieczni? Może nigdy?
  - Ile jestem w stanie wydać na bezpieczeństwo?
    - Samochody meteoroodporne?
- Użyteczność/Dostępność vs Bezpieczeństwo
  - Czy SSO zwiększa czy zmniejsza bezpieczeństwo?
- Prywatność vs Bezpieczeństwo
  - Im więcej wiemy tym większa szansa że się uchronimy?
    - CBA?
- Swoboda vs Bezpieczeństwo
  - "*Ci którzy chcieli by oddać podstawy wolności, by kupić trochę czasowego bezpieczeństwa, nie zasługują ani na wolność ani na bezpieczeństwo*."
    Benjamin Franklin

Kilka faktów

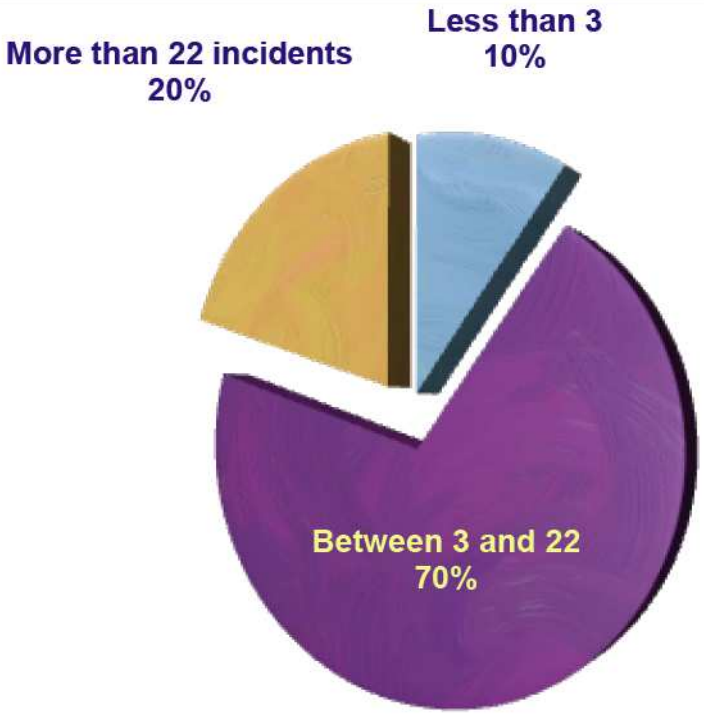


Ilość usług zewnętrznych w latach 2003-2008 wzrosła 700%

Kilka faktów

Security Requirements

Breaches of sensitive business data in past year:

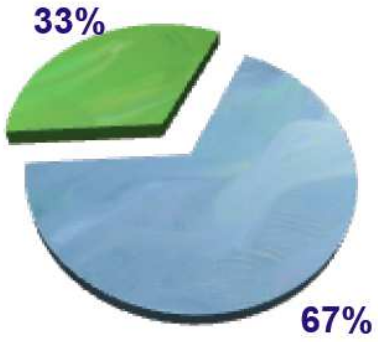


Source: 2006,07,08 survey by the IT Policy Compliance Group

Kilka faktów

Improper Use of Corp Data

- 59% of workers who left their positions took confidential information with them
- 67% used their former company's confidential information to leverage a new job



Time to terminate access

- 24% still had access to Corporate Systems

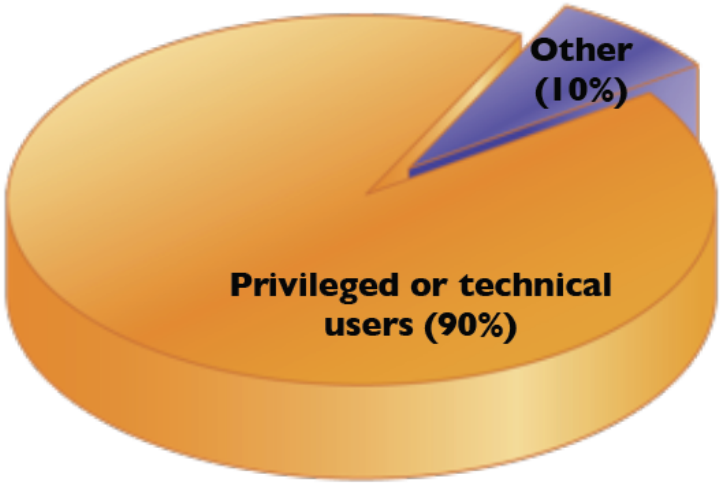
Source: "Data Loss Risks During Downsizing", Ponemon Institute LLC,Feb 23, 2009

Kilka faktów

The enemy is "us":

- **90% of insider incidents are caused by privileged or technical users**
- **Most are inadvertent violations of:**
  - Change management process
  - Acceptable use policy
  - Account management process
- **Others are deliberate, due to:**
  - Revenge (84%)
  - "Negative events" (92%)
- **Regardless, too costly to ignore:**
  - Internal attacks cost 6% of gross annual revenue or 9 dollars per employee per day

What causes Internal Incidents?



Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005/6; CSI/FBI Survey, 2005; National Fraud Survey; CERT, various documents.

Kilka faktów

Operator Error
60%

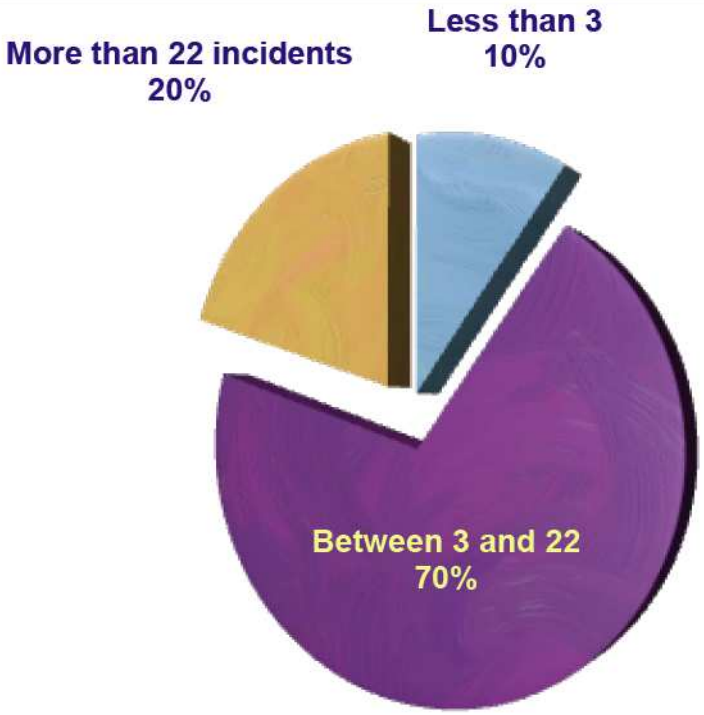
Malicious Attacks
20%

Application Failure
20%

Kilka faktów

Security Requirements

Breaches of sensitive business data in past year:



Source: 2006,07,08 survey by the IT Policy Compliance Group

Nowości w TS

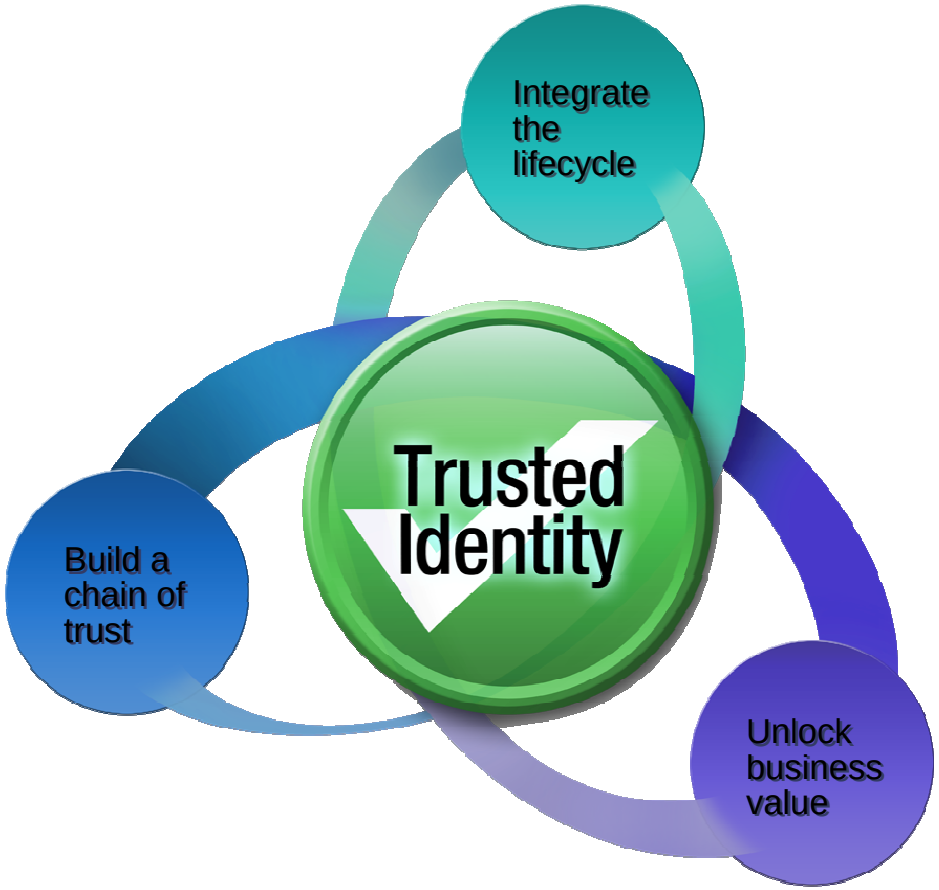
- TDI 7.0 (GA)
  - Nowy interfejs – Eclipse
  - Szybciej, czytelniej, sprawniej
- TIM 5.1 (GA)
  - SoD – segregacja uprawnień
  - Nowy system recertyfikacji
  - Hierachiczne role
  - Zarządzanie grupami
- TAMESSO 8.1
  - Generyczne wsparcie PKI
  - Firefox 2.x, 3.x
  - Windows Vista i 2008
- TKLM (GA)
- TSIEM 2.0

Zarządzanie tożsamością i dostępem

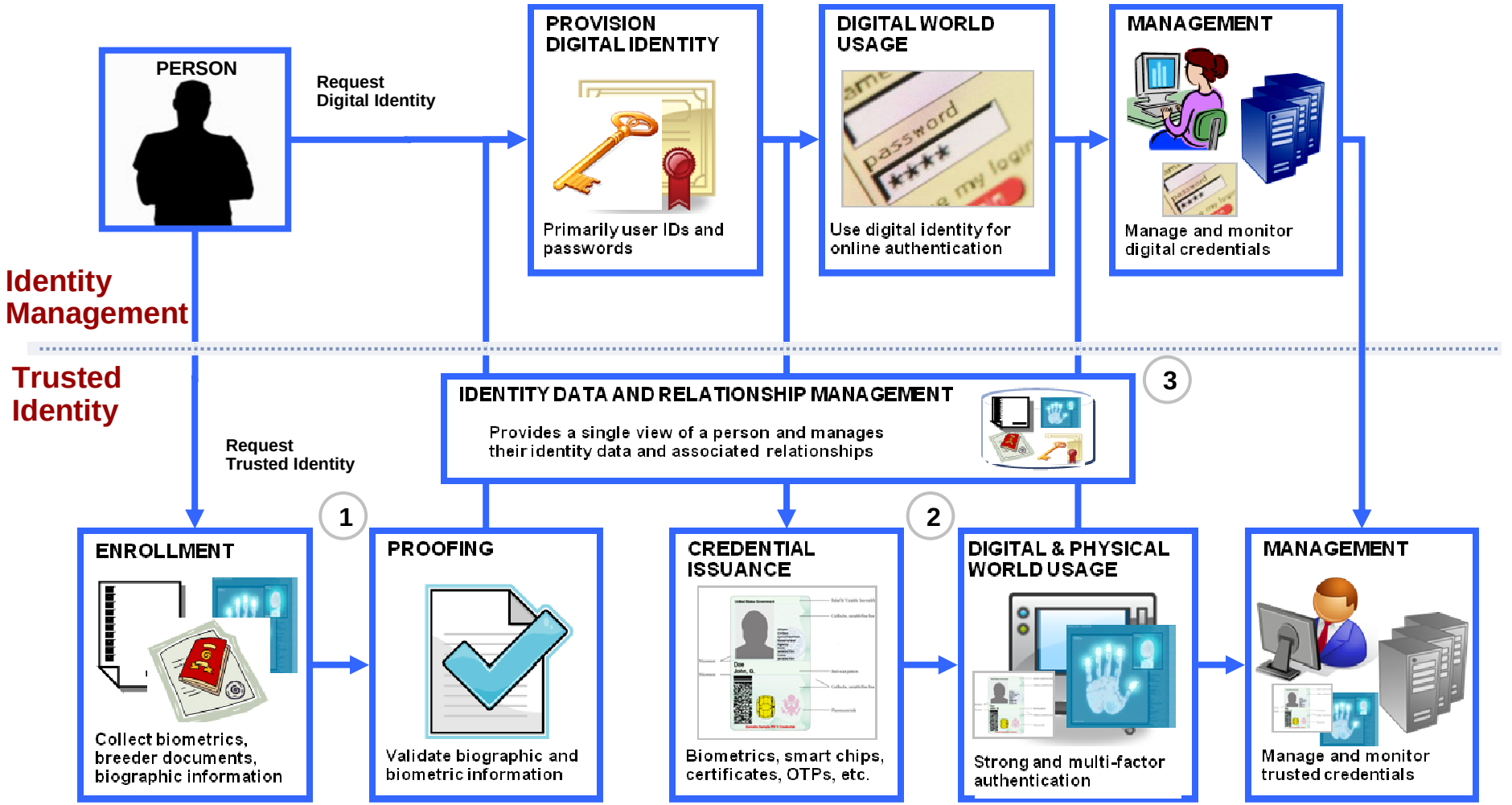
Zarządzanie
KTO ma DOSTĘP do CZEGO
i DLACZEGO

Ludzie	Polityki	Zasoby

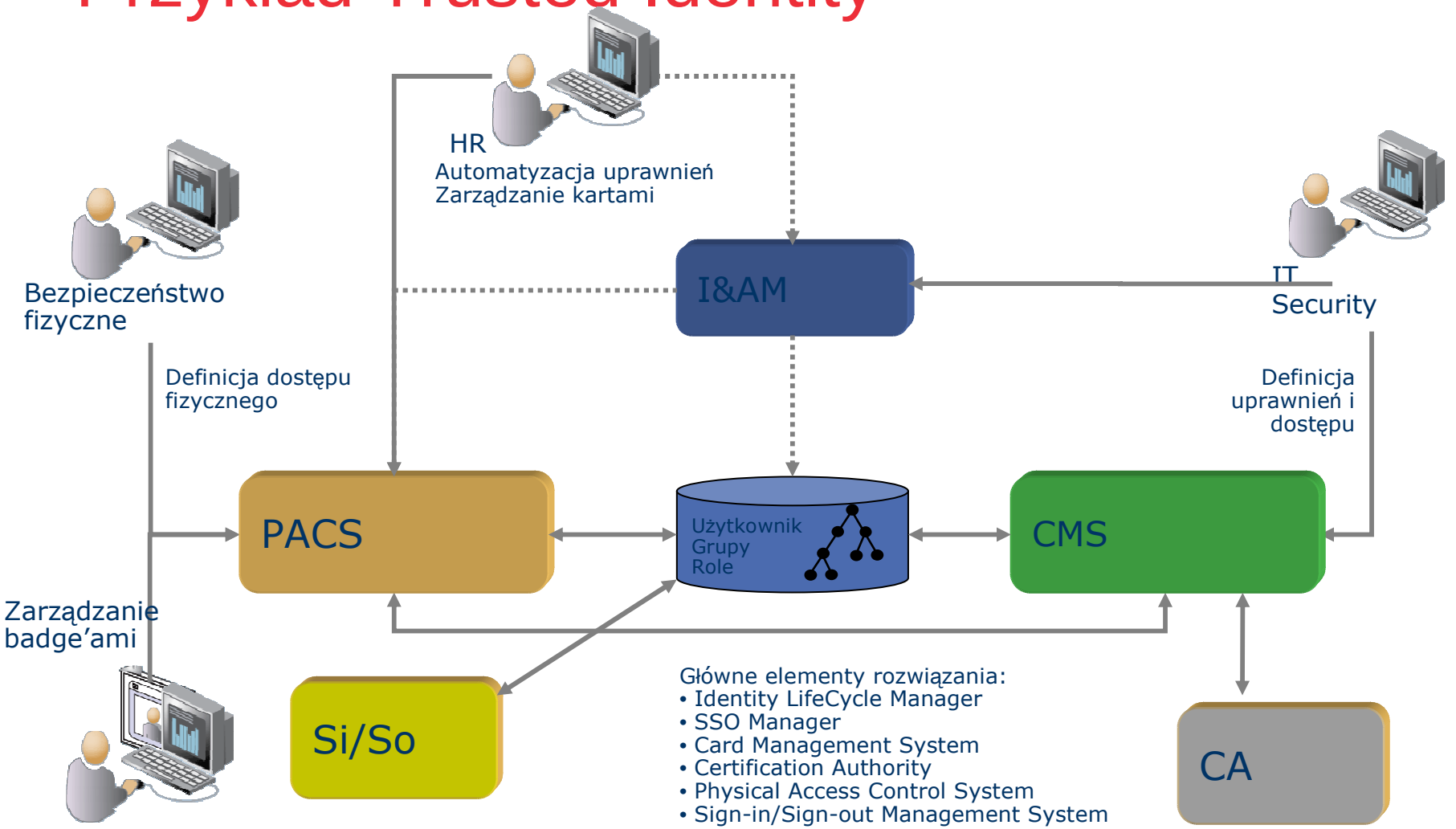
Trusted Identity



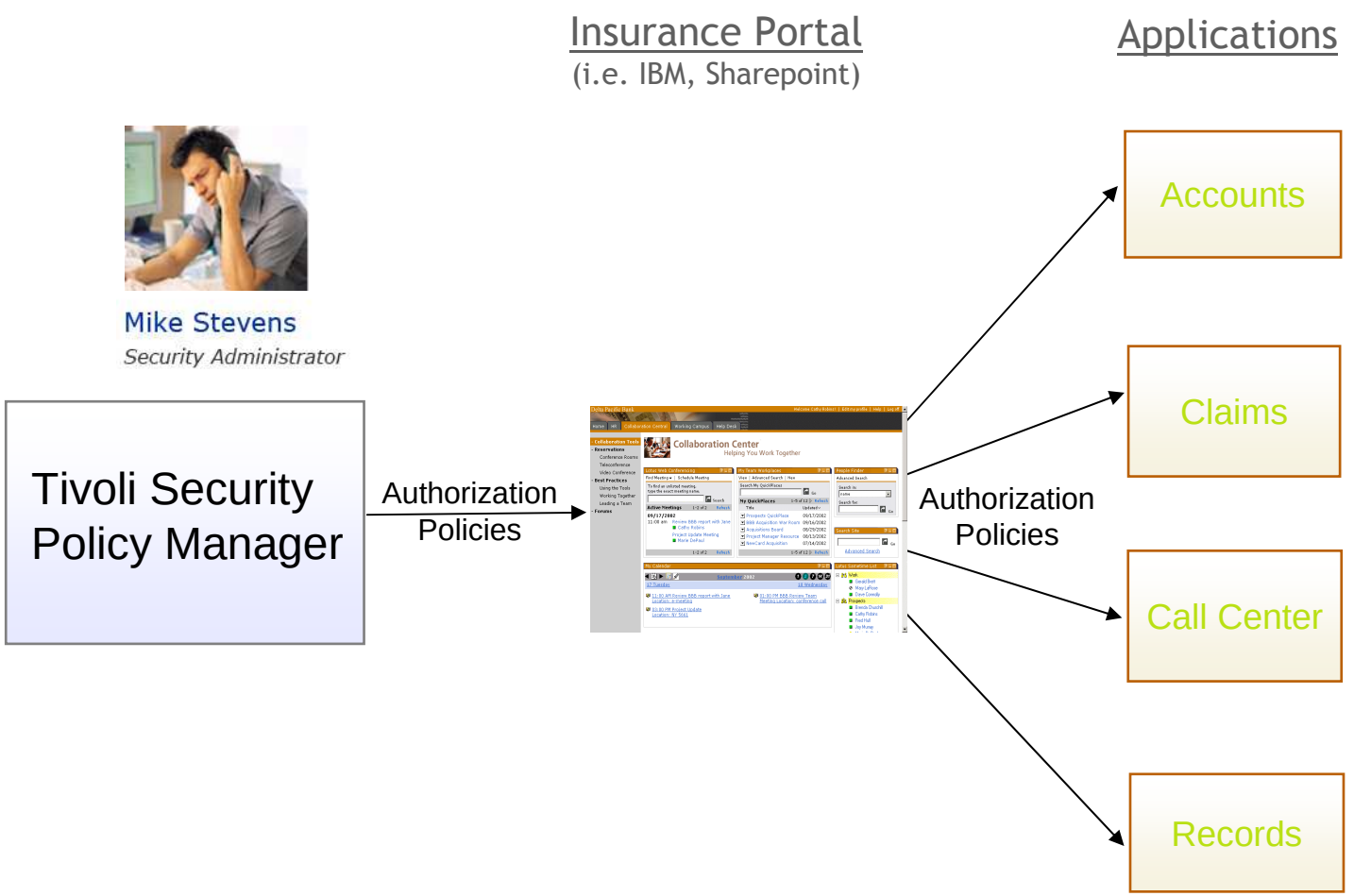
Identity Management vs. Trusted Identity



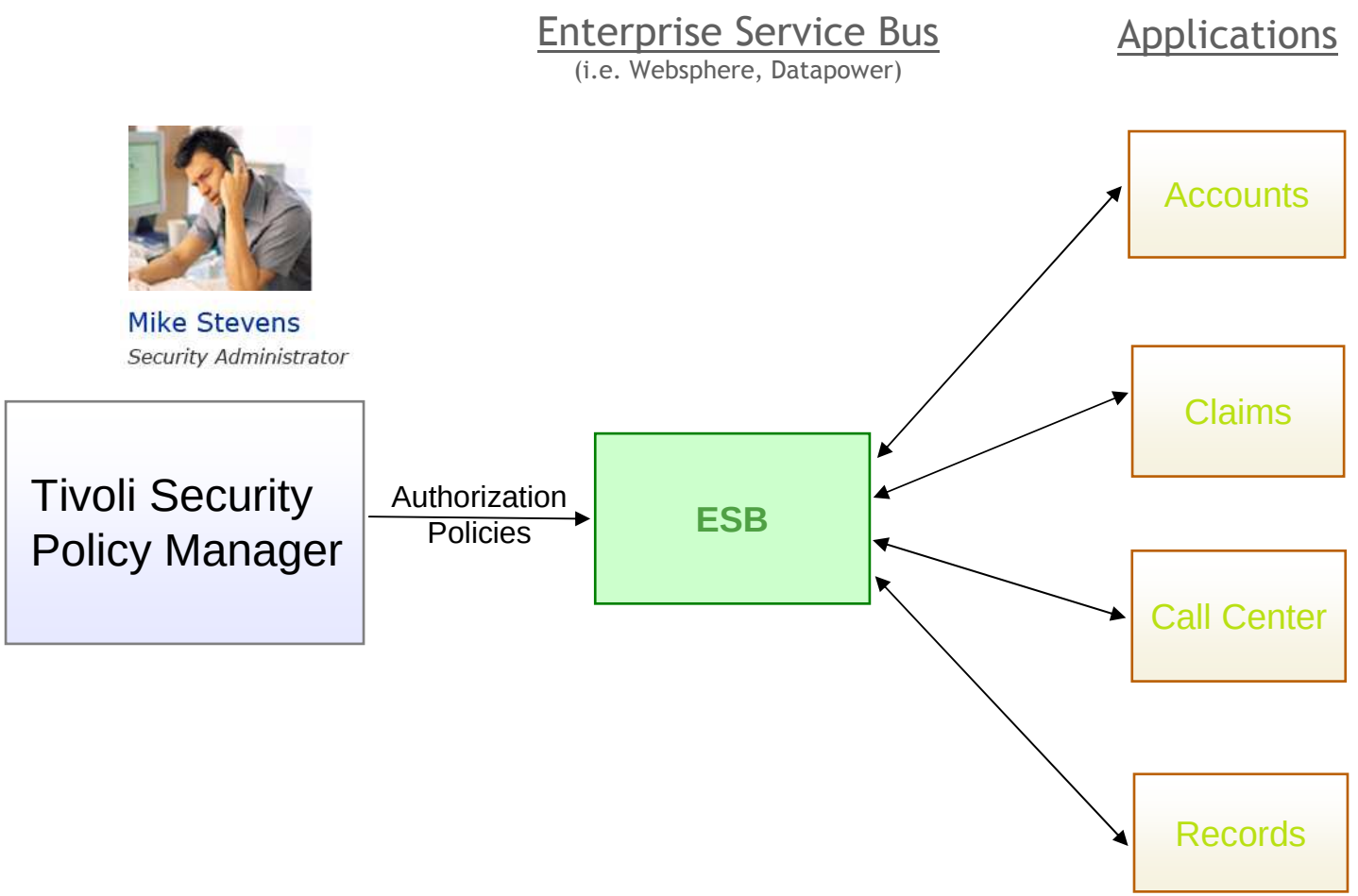
Przykład Trusted Identity



TSPM Solution – Portal Deployment Project



TSPM Solution – ESB Project



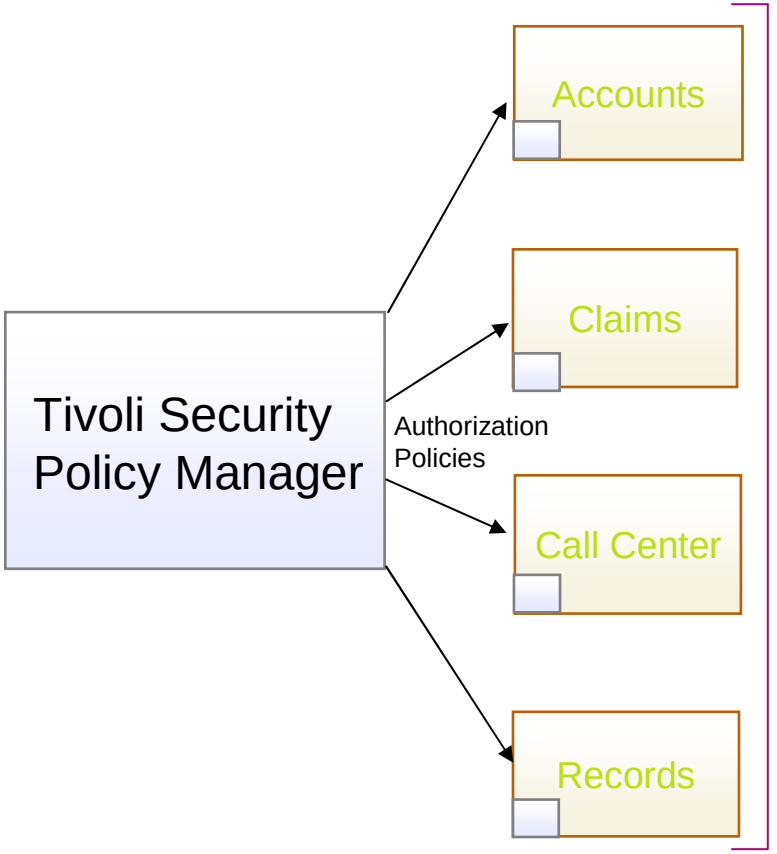
TSPM Data & Application Security

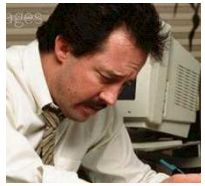
Mike Stevens
Security Administrator

Determines data access policies based on business and compliance drivers and provides to Jose.

Example policy:

- Claims Approver can view all claims but only approve their own claims and if the value is less than 25% of the insured value.





Jose Fuentes
Application Programmer

How many levels of access granularity does Jose need to code?

?

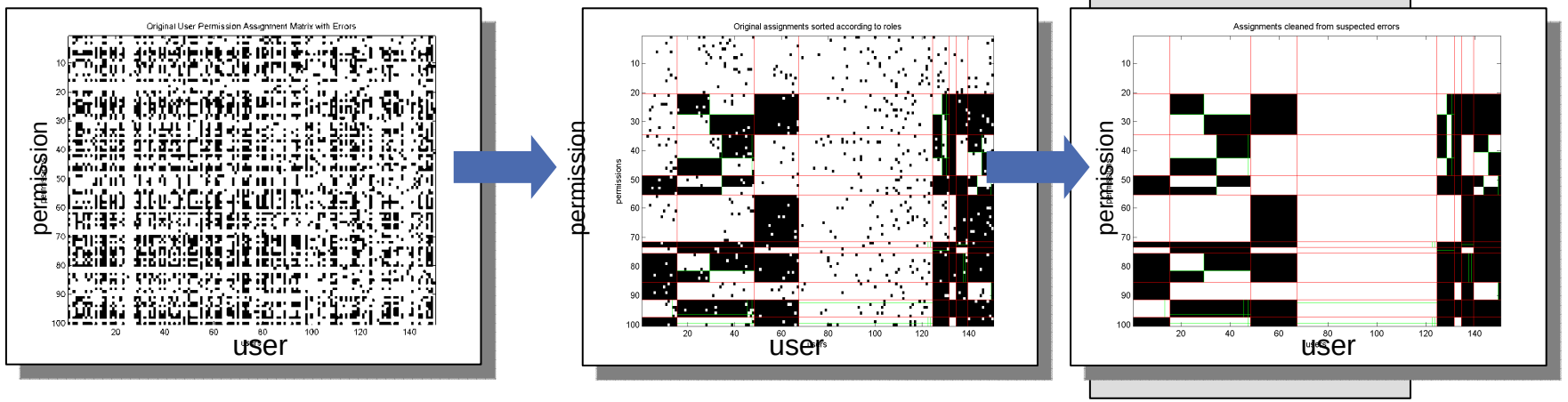
Authorization Policies coded into application

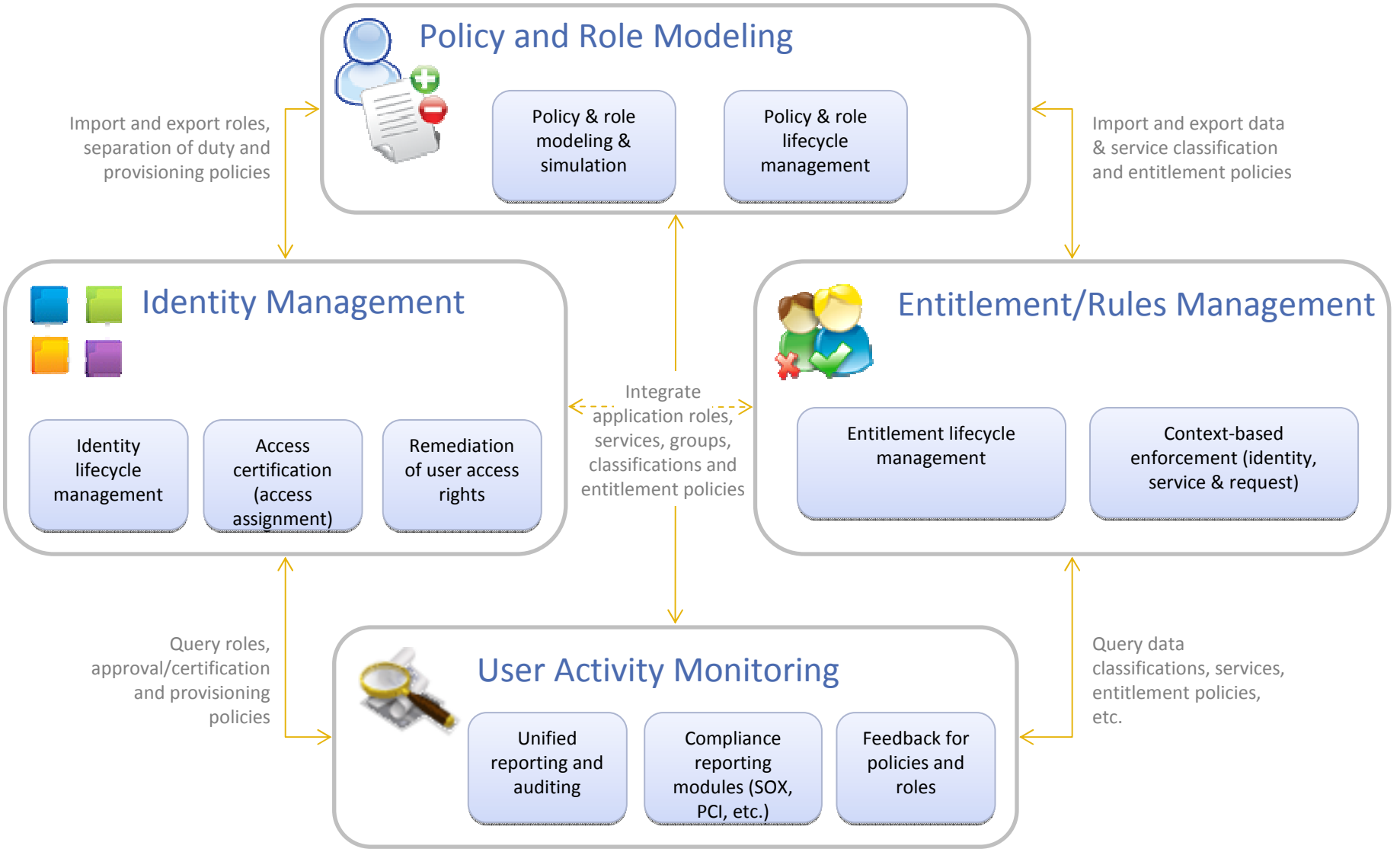
Zarządzanie poprzez role

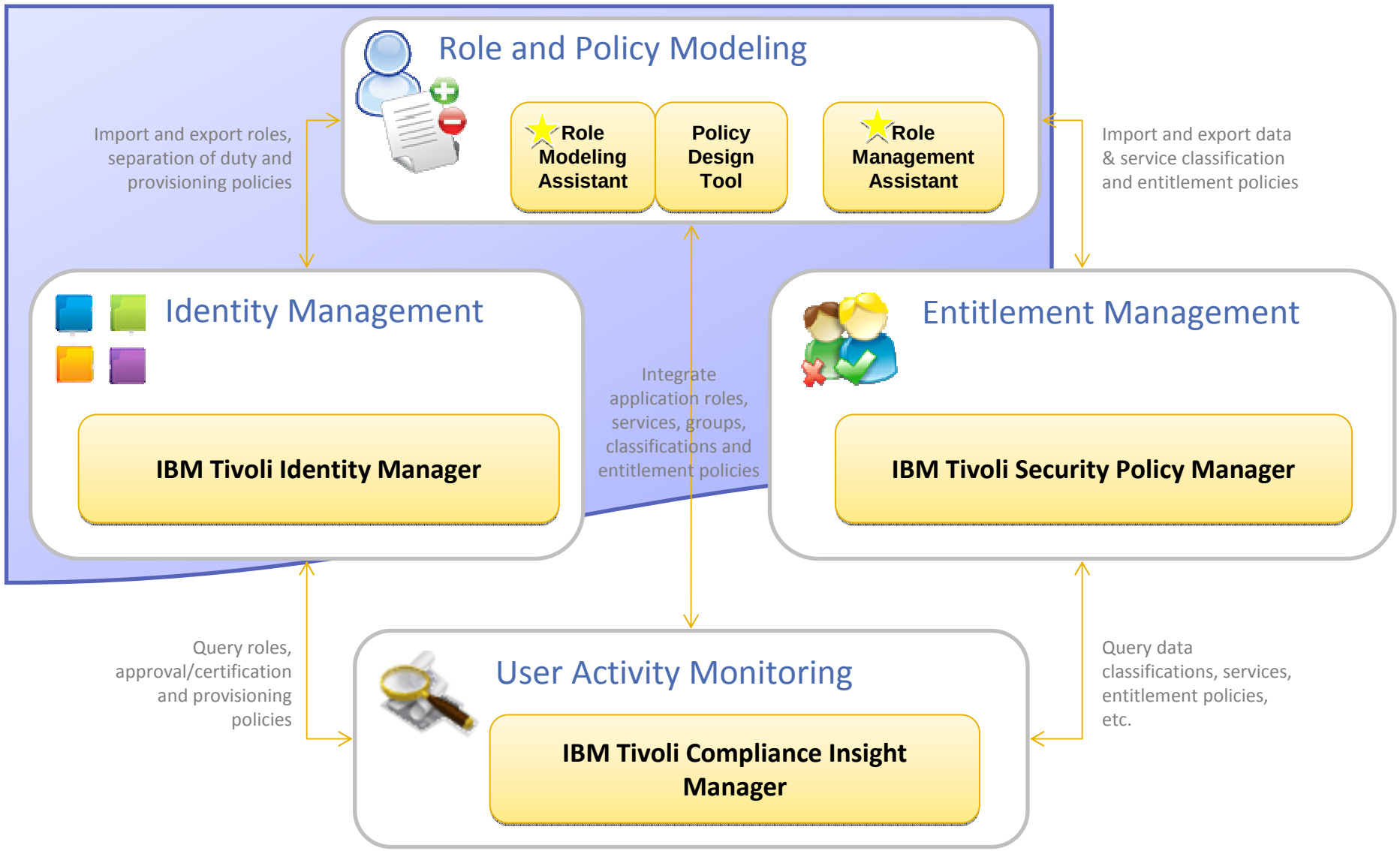
Istniejące uprawnienia w systemach

Uprawnienia po analizie i usunięciu błędów

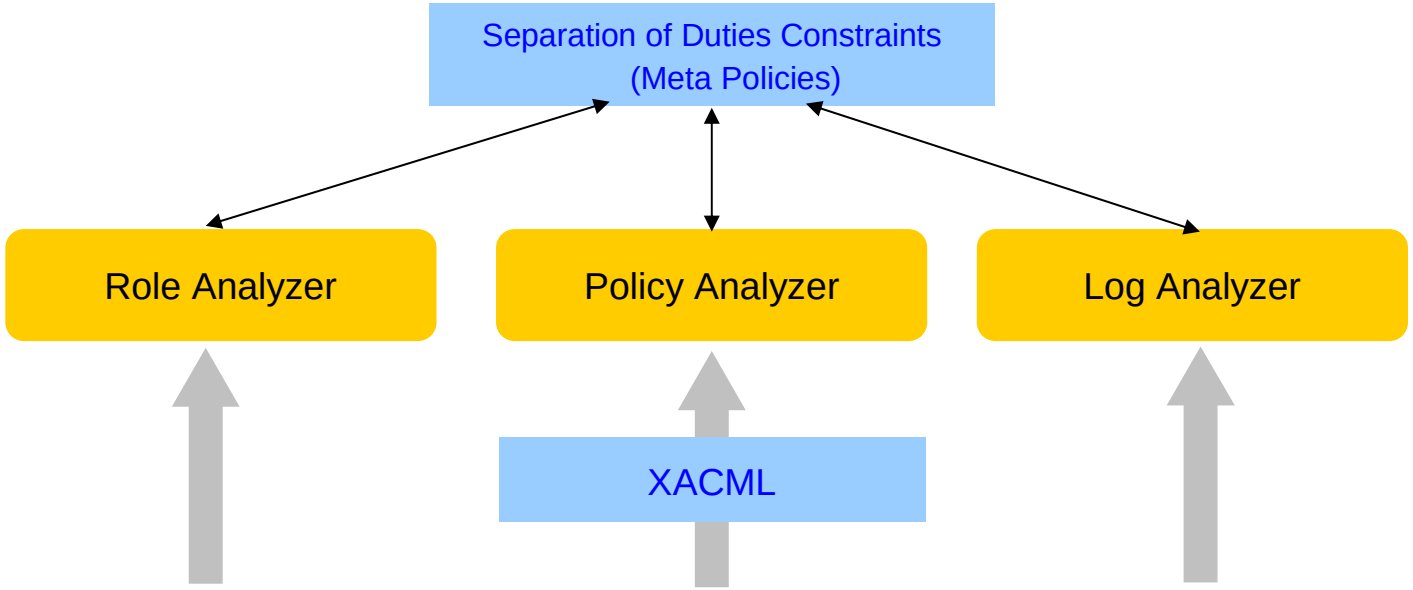
Wyczyszczone role




Policy and Role Modeling
Policy & role modeling & simulation
Policy & role lifecycle management
Import and export roles, separation of duty and provisioning policies
Import and export data & service classification and entitlement policies
Identity Management
Identity lifecycle management
Access certification (access assignment)
Remediation of user access rights
Integrate application roles, services, groups, classifications and entitlement policies
Entitlement/Rules Management
Entitlement lifecycle management
Context-based enforcement (identity, service & request)
Query roles, approval/certification and provisioning policies
User Activity Monitoring
Unified reporting and auditing
Compliance reporting modules (SOX, PCI, etc.)
Feedback for policies and roles
Query data classifications, services, entitlement policies, etc.


Role and Policy Modeling
Role Modeling Assistant
Policy Design Tool
Role Management Assistant
Import and export roles, separation of duty and provisioning policies
Import and export data & service classification and entitlement policies
Identity Management
IBM Tivoli Identity Manager
Integrate application roles, services, groups, classifications and entitlement policies
Entitlement Management
IBM Tivoli Security Policy Manager
Query roles, approval/certification and provisioning policies
User Activity Monitoring
IBM Tivoli Compliance Insight Manager
Query data classifications, services, entitlement policies, etc.

SoD


Separation of Duties Constraints
(Meta Policies)
Role Analyzer
Policy Analyzer
Log Analyzer
XACML

Boundles

Identity & Access Assurance	→	**Reduce cost and risk by easing the onboarding and offboarding of users, reporting on user activity and ongoing access certification**
Data & Application Security	→	**Protect business information and reputation by safeguarding data in use or at rest**
Security Management for System z	→	**Improve mainframe security administration & enable integrated mainframe & distributed security workloads**