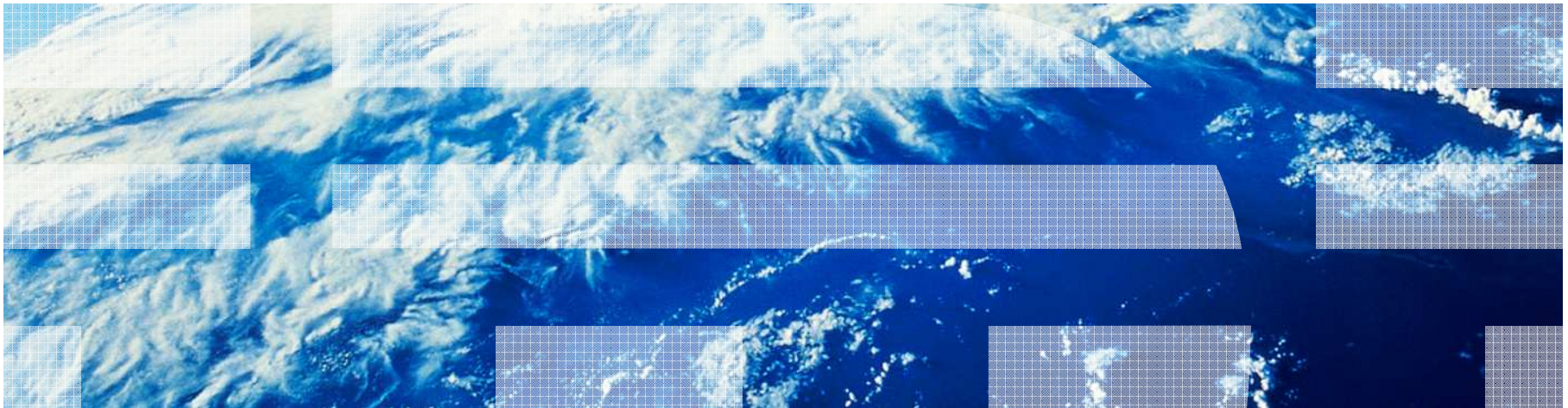


IBM Security Framework: Identity & Access management, potreby a riešenia.



Nová doba – inteligentná infraštruktúra

Globalizácia a globálne dostupné zdroje

Miliardy mobilných zariadení s prístupom na internet

Prístup k informáciám v reálnom čase



Nové formy komunikácie

Tvárou v tvár:

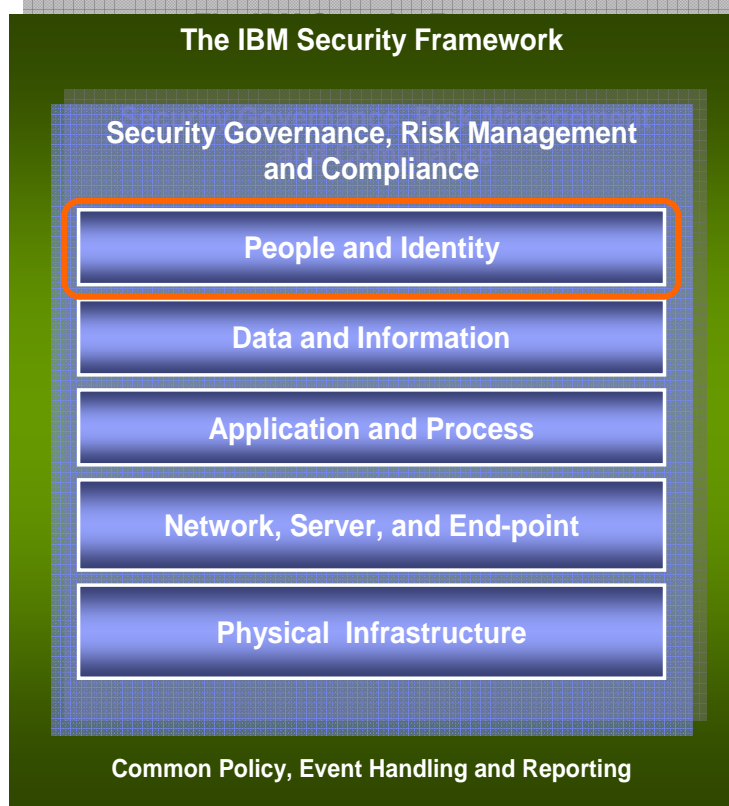
Novým možnostiam
Novej komplexnosti
Novým rizikám

Pomáhame:

Zlepšovať Služby
Redukovať Náklady
Riadiť Riziká

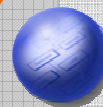
IBM Security Framework

IBM Security Solutions



SECURITY COMPLIANCE

- Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)



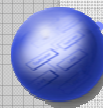
IDENTITY & ACCESS

- Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets



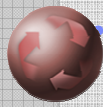
DATA SECURITY

- Protect and secure your data and information assets



APPLICATION SECURITY

- Continuously manage, monitor and audit application security



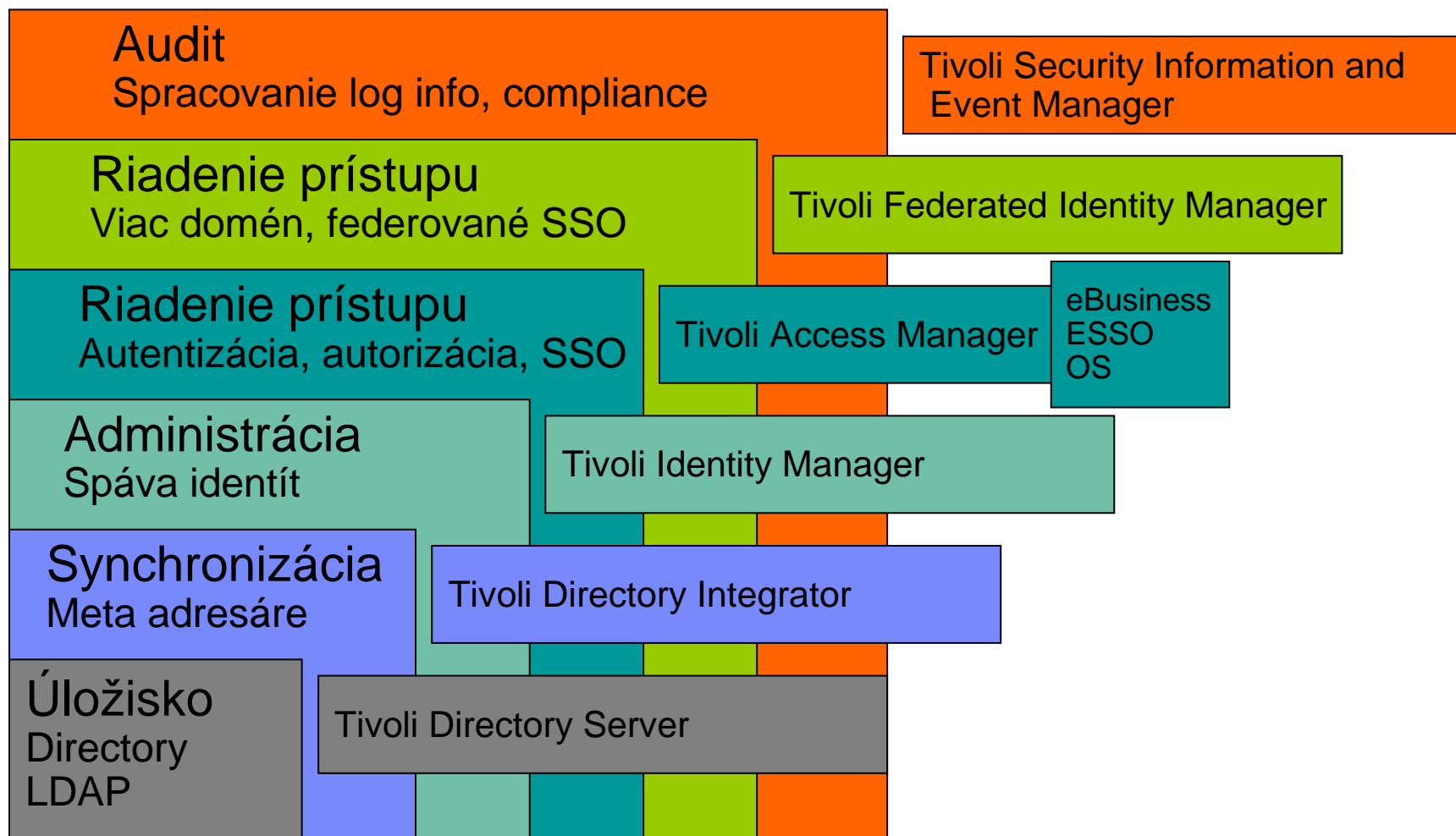
INFRASTRUCTURE SECURITY

- Comprehensive threat and vulnerability management across networks, servers and end-points

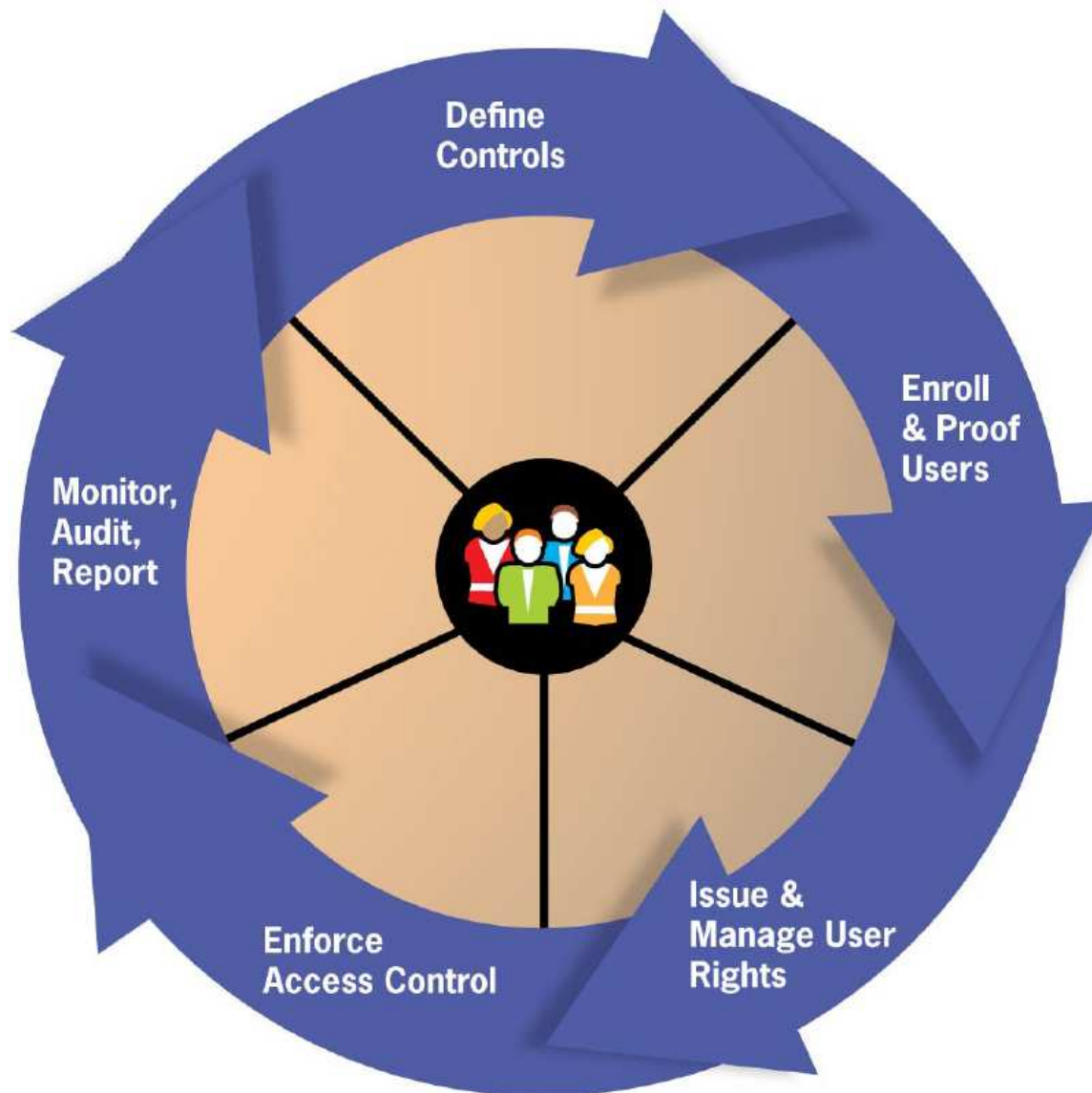
Tivoli Security Product Abbreviation Guide / Cheat Sheet

TAM E-SSO	Tivoli Access Manager for Enterprise Single Sign-On	Enterprise SSO
TAMeb	Tivoli Access Manager for e-business	Web SSO/access control
TAMOS	Tivoli Access Manager for Operating Systems	UNIX/Linux access control
TCIM	Tivoli Compliance Insight Manager	Audit management/reporting
TDI	Tivoli Directory Integrator	Synchronize info across repositories
TDS	Tivoli Directory Server	Scalable/available (often embedded) LDAP
TFIM	Tivoli Federated Identity Manager	Identity transform – SOA and federated
TFIM BG	Tivoli Federated Identity Manager Business Gateway	TFIM “Lite”
TIM	Tivoli Identity Manager	User provisioning, recertification, pw synch, ...
TKLM	Tivoli Key Lifecycle Manager	Crypto key management
TSCM	Tivoli Security Compliance Manager	Server/workstation policy setting/enforcement
TSIEM	Tivoli Security Information and Event Manager	Event/audit management/reporting
TSOM	Tivoli Security Operations Manager	24x7 security operations center
TSPM	Tivoli Security Policy Manager	Entitlement and SOA policy management

Riadenie identít a prístupov



Cyklický proces riadenia identít a prístupov



Typické problémy Identity Managementu

- Vytváranie nových používateľov

Povolenie prístupov používateľovi trvá až 12 dní

- Podpora používateľov

Vysoké náklady na resetovanie hesiel

- Odstraňovanie nepotrebných účtov

30-60% existujúcich účtov je neplatná

- Tvorba nových aplikácií

Až 30% času vývoja aplikácie sa týka prístupov

Identity Management

Riadenie
KTO má ***PRÍSTUP*** ku ***ČOMU***

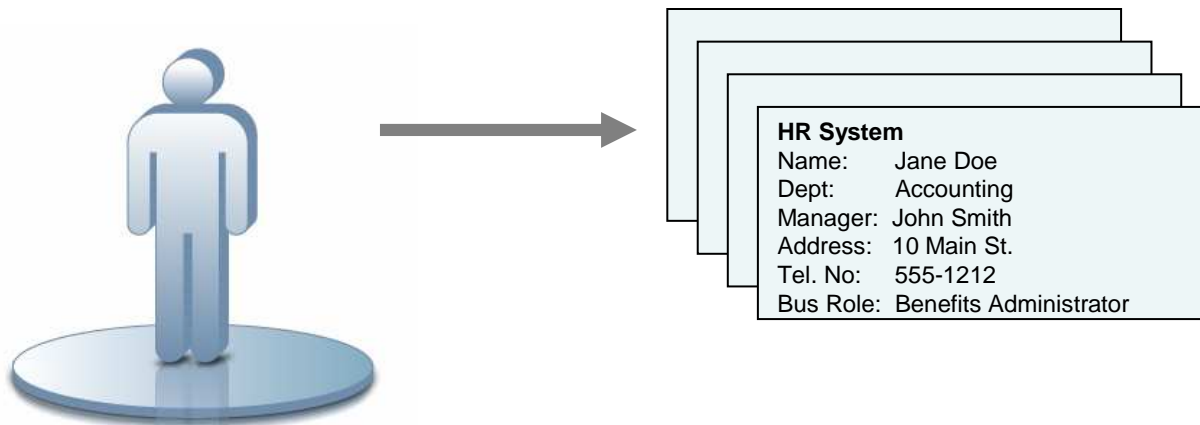


KTO v Identity Managemente

- Používatelia definovaní v Identity Managemente sú ľudia, ktorí potrebujú prístup ku zdrojom.

- Používatelia môžu byť **interní** alebo **externí**

- Zamestnanci
- Zákazníci
- Obchodní partneri
- Občania
- ...



- Každý používateľ má **identitu** a **atribúty**.
- Atribútom používateľa môže byť jeho **rola**.

ČO v Identity Managemente

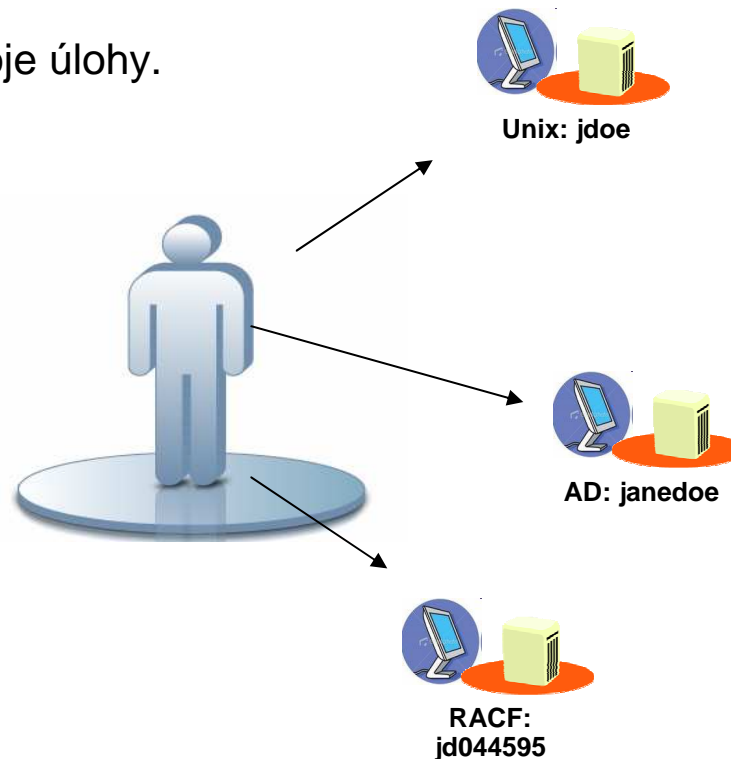
- ČO je používateľský účet na IT zdroji.
- Účet je potrebný, aby používateľ mohol vykonávať svoje úlohy.
- Prístup je zabezpečený prostredníctvom účtu.

- Príklady zdrojov

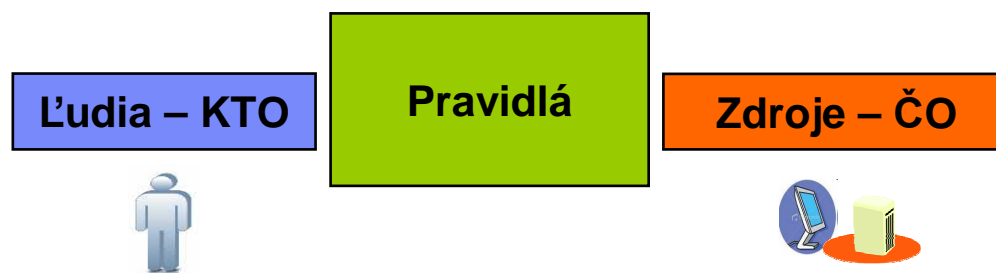
- Operačný systém
- Databáza
- Aplikácia
- Adresár

Windows, Linux, Unix
DB2, MS SQL, Oracle
Lotus Notes, SAP
Active Directory

- Účet bežne pozostáva z
 - userid
 - heslo
 - skupina alebo rola

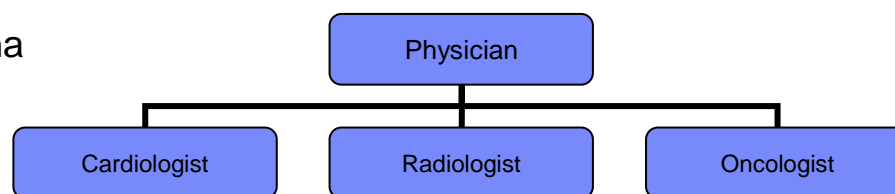


Ako je zabezpečený *PRÍSTUP*

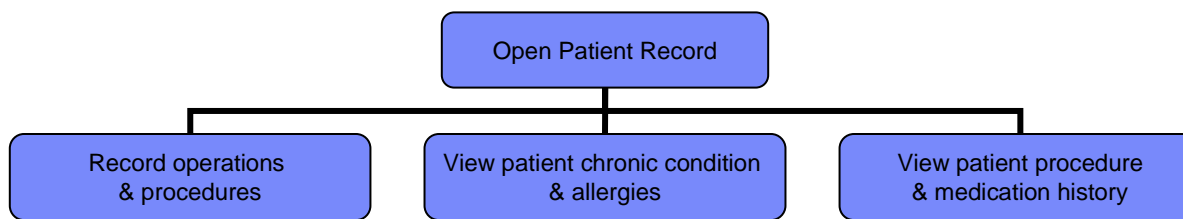


- Pravidlá definujú, kto má **PRÍSTUP** ku zdrojom
- Pravidlá pozostávajú z členstva a oprávnení
- **Schvaľovací proces** zabezpečí pridelenie prístupu správnym ľuďom ku správnym zdrojom
- Príslušnosť ku pravidlám môže byť definovaná na základe **rolí**

– business rola

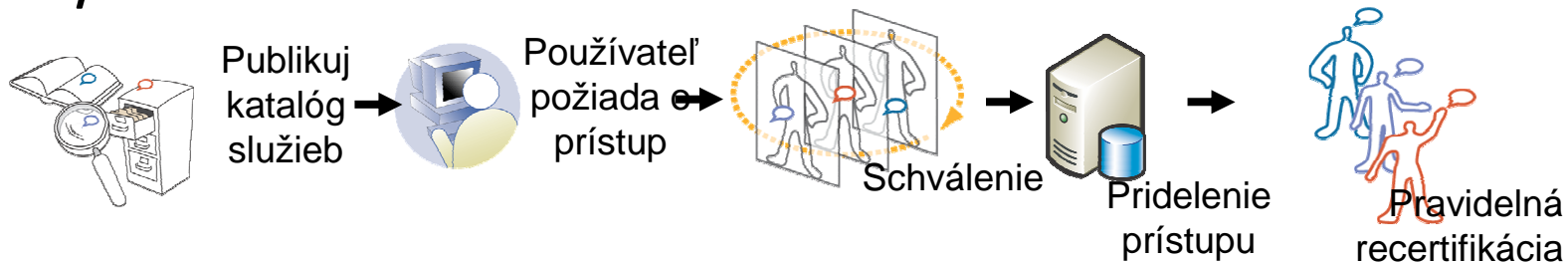


– aplikačná rola

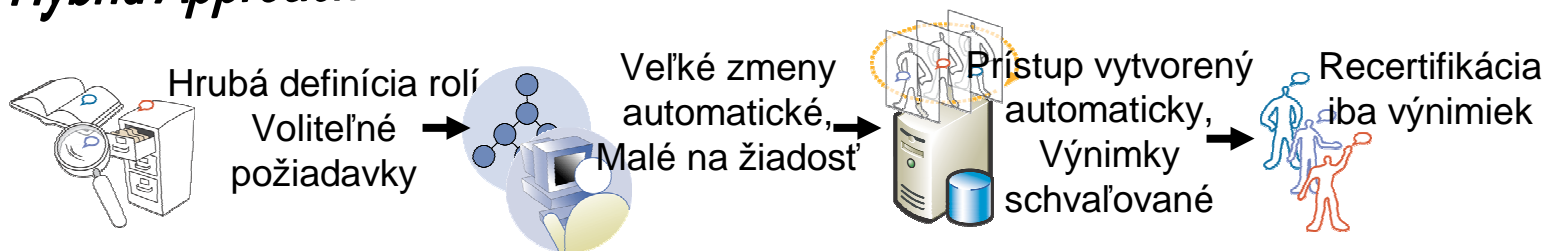


Možnosti automatickej správy prístupov

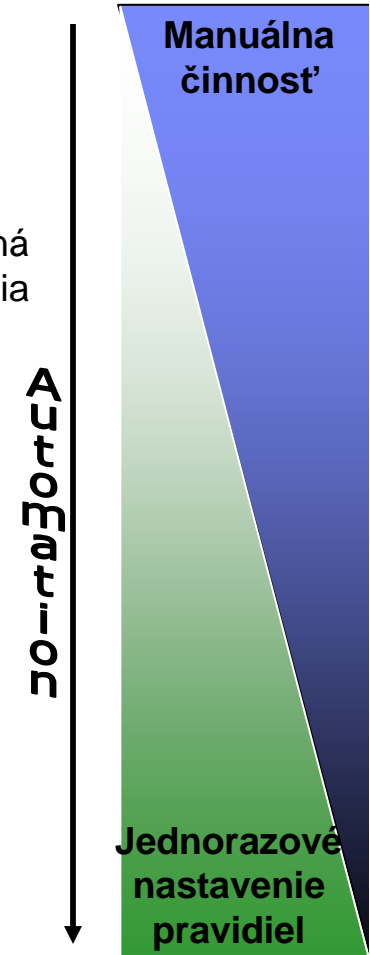
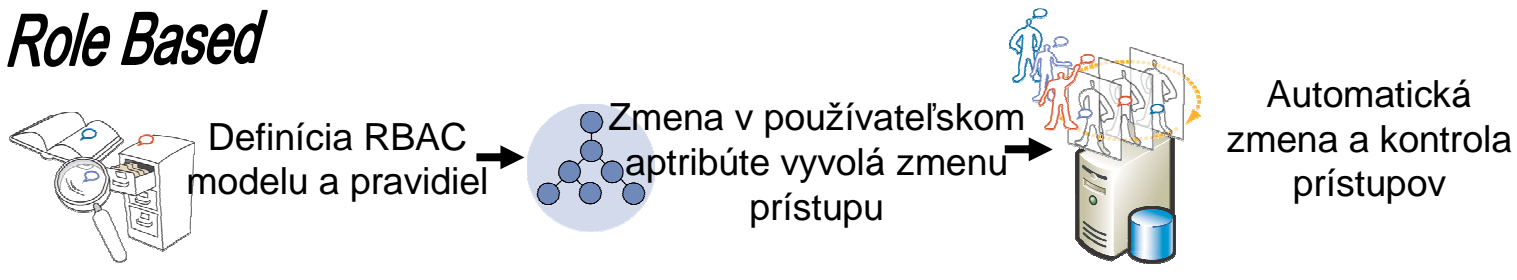
Request Based



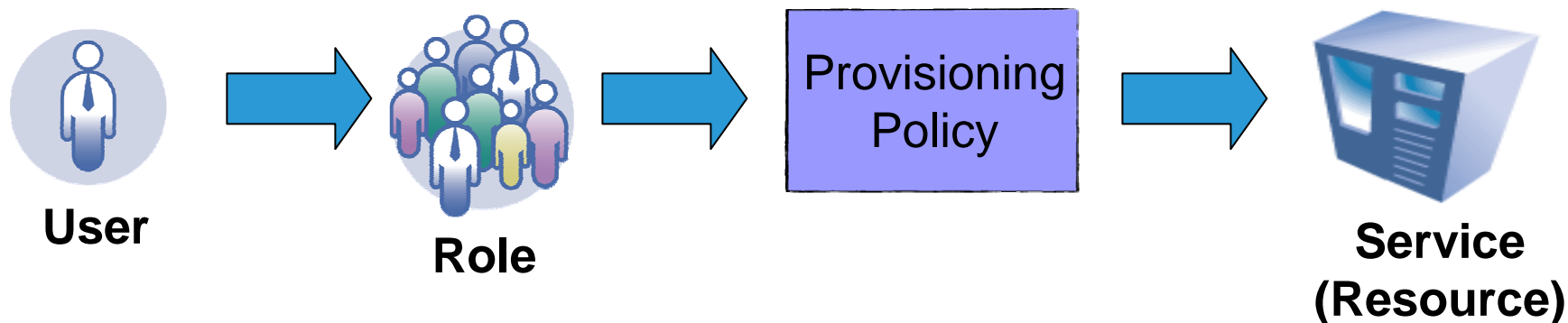
Hybrid Approach



Role Based

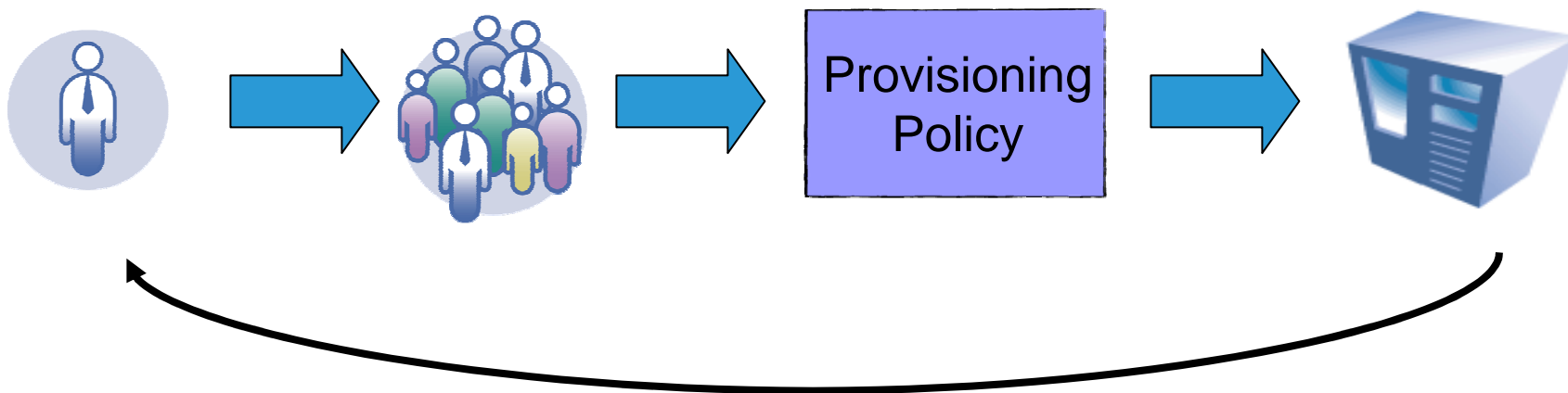


Postup vytvorenia prístupu



- Používateľ má priradenú rolu podľa svojej pracovnej náplne
- Na základe role sú vytvorené prístupy ku zdrojom podľa definovaných pravidiel
- Pravidlá môžu nastavovať atribúty používateľov

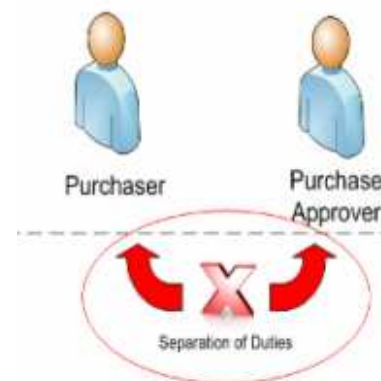
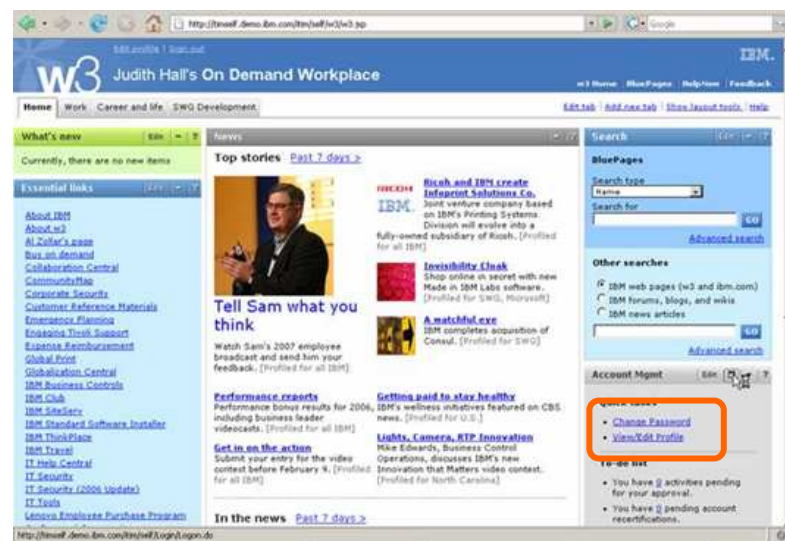
Zusúladenie „Čo je“ oproti „Čo má byť“ - reconciliation



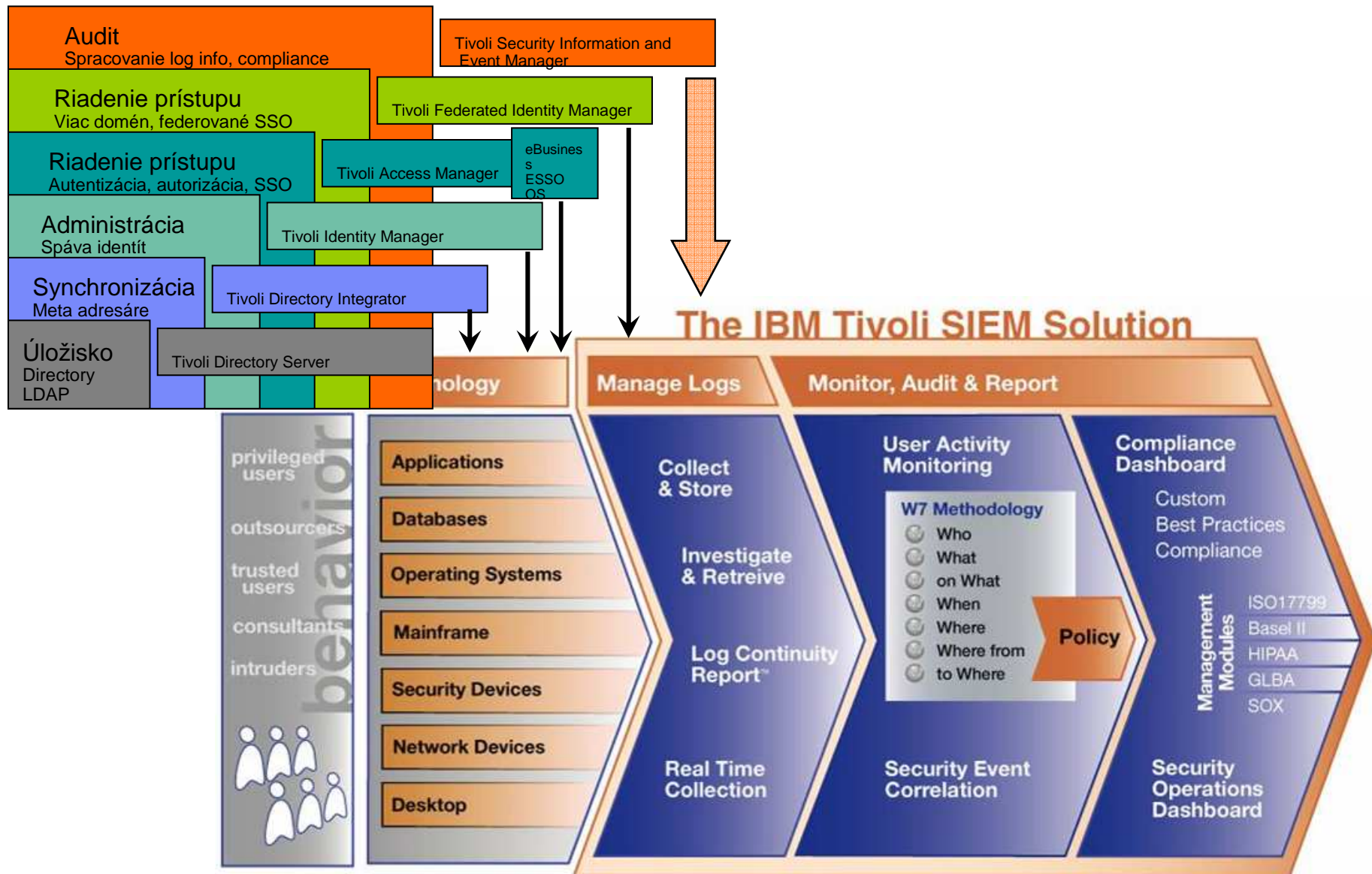
- Vynútenie nastavenie podľa definovaných pravidiel
- Tivoli Identity Manager môže modifikovať neautorizované zmeny:
 - Rollback
 - Accept
 - Suspend
- Identifikácia nevyužívaných účtov

Ďalšie možnosti Tivoli Identity Manager

- Samo-obsluha (reset hesla, úprava profilu ...)
- Integrovaťnosť rozhrania do vlastného prostredia
- Rozdelenie právomocí (Separation of Duties)
- Integrácia so Single Sign-On
- ...



Bezpečnostný audit a sledovanie log-súborov



Čo na to analytici?

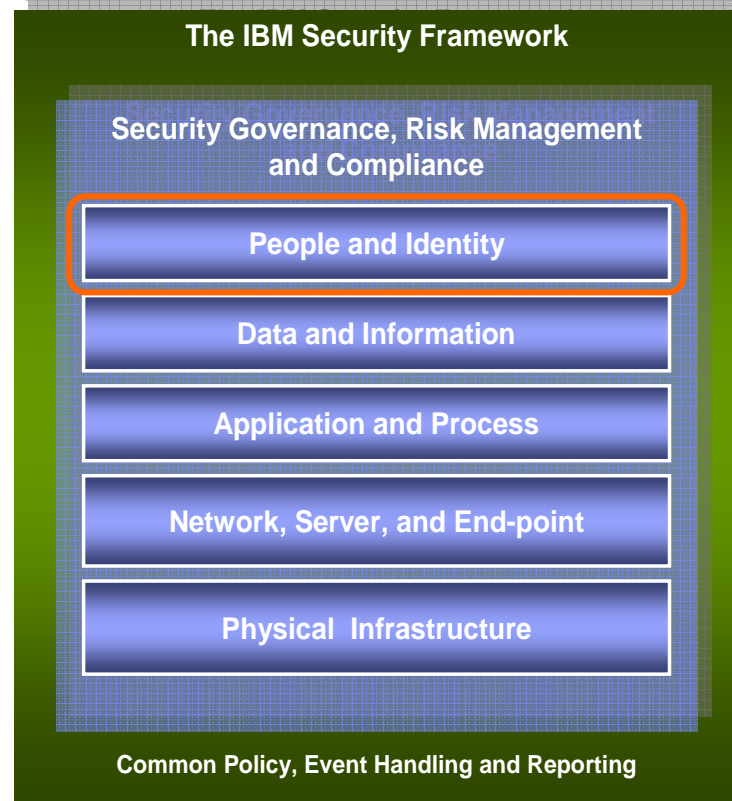
**Security Project Portfolio Placement
(Listed in "Top 5" Priorities)**

**Top Security Project Priority
(Listed as No. 1 Project)**

Ranking			Ranking		
1	Intrusion Prevention	47.5%	1	Identity Management	20.5%
2	Patch Management	46.1%	2	Data Loss Prevention	13.9%
3	Data Loss Prevention	44.5%	3	Antivirus	10.6%
4	Antivirus	41.1%	4	Firewalls	9.3%
4	Identity Management	41.1%	5	Intrusion Prevention	8.6%
6	Firewalls	37.4%	6	Network Access Control	7.3%
6	Vulnerability Assessment	37.4%	6	Patch Management	7.3%
8	Network Access Control	35.5%	8	Security Information and Event Management	5.3%
8	Security Information and Event Management	35.5%	9	Strong User Authentication	4.6%
10	Remote-Access or Site-to-Site VPN	31.2%	10	Remote-Access or Site-to-Site VPN	4.0%

The IBM Security Framework

- IBM je dodávateľom komplexných riešení – technológií i služieb
- IBM Global Technology Services má na Slovensku tím ľudí, ktorí sa zaoberajú bezpečnosťou
- Máme lokálne skúsenosti s implementáciou IAM riešení postavených na štandardnom produkte, aj s riešeniami na kľúč



IBM Security Solutions

- SECURITY COMPLIANCE
- IDENTITY & ACCESS
- DATA SECURITY
- APPLICATION SECURITY
- INFRASTRUCTURE SECURITY

Otázky a odpovede

