Prima di cominciare…

Identità Digitale: tra Sicurezza e Privacy

(a cura di **Massimo Cipriani**)

Agenda

Generalità

Identità ed identificativi

Conformità normativa

Piattaforma di IM

Riferimenti bibliografici e sitografici

Varie – Q&A

Identità

"Ogni essere umano è unico. In tutto il mondo non si possono trovare due esseri umani perfettamente identici. Persino i veri gemelli manifestano delle differenze. La particolarità dell'uomo è proprio quella di avere un'identità che non definisce nessun altro che lui. È unico, cioè irripetibile."

da "Il razzismo spiegato a mia figlia"
Tahar Ben Jelloun

- la privacy individuale senza la quale l'individuo non può più essere tale e senza la quale individualità egli non è più nulla che valga la pena continuare a essere -

da "Privacy"
William Faulkner

Identità

- Cos'è la nostra identità? Essa è tutto ciò che caratterizza ciascuno di noi come individuo singolo e inconfondibile. E' ciò che impedisce alle persone di scambiarci per qualcun altro. Così come ognuno ha un'identità per gli altri, ha anche un'identità per sé. Quella per gli altri è l'identità oggettiva, l'identità per sé è l'identità soggettiva. L'identità soggettiva è l'insieme delle mie caratteristiche così come io le vedo e le descrivo in me stesso. L'identità oggettiva di ciascuno, ossia la sua riconoscibilità, si presenta secondo tre principali modalità. La prima modalità è l'identità fisica: questa è data soprattutto dalle caratteristiche della faccia, le quali ci permettono di non esser confusi con un'altra persona. La seconda modalità è l'identità sociale, ossia un insieme di caratteristiche quali l'età, lo stato civile, la professione, il livello culturale e l'appartenenza ad una certa fascia di reddito. La terza modalità è l'identità psicologica, ovvero la mia personalità, lo stile costante del mio comportamento ...

- L'identità personale soprattutto è il risultato di una somma di differenze fisiche, caratteriali, di storia personale, culturali, ognuna delle quali concorre a fare di ciascuno un essere assolutamente unico.

Identità e attributi

Identità

Attributi

Nome

Cognome

Luogo e Data di nascita

Indirizzo

Codice Fiscale

Stato civile

Società di appartenenza

Ruolo aziendale

…

Identità digitale

L'**identità digitale** è l'insieme delle informazioni che descrivono univocamente una persona (o un dispositivo) chiamata *soggetto* o *entità,* e contiene anche informazioni relative alle relazioni del soggetto con altre entità.

identità o identificativo?

Identità digitale

- Un *soggetto* o *entità* è una persona, un'entità organizzativa, un programma software, un sistema o qualsiasi altra cosa che richiede l'accesso ad una risorsa.

- Una *risorsa* può essere una pagina web, un campo di un database o anche una transazione con una carta di credito.

- Per ottenere l'accesso ad una risorsa, il soggetto si basa sull'ottenimento di un'*identità*.

Identità, Sicurezza e Privacy: relazioni tra gli elementi

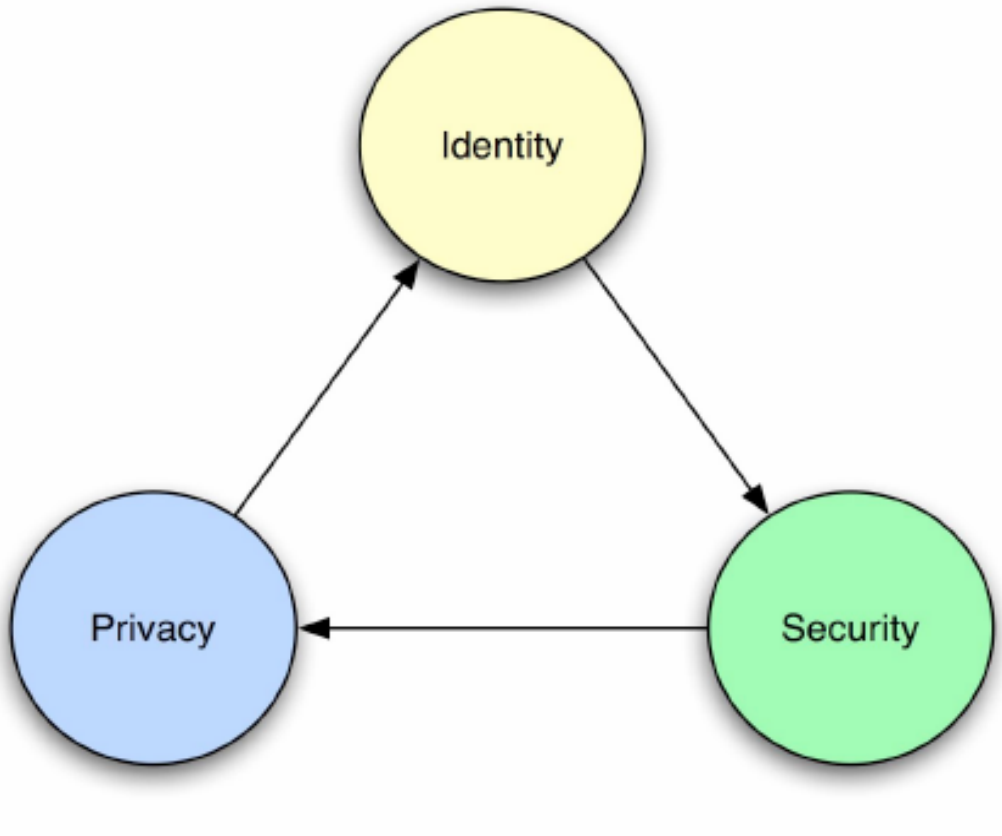
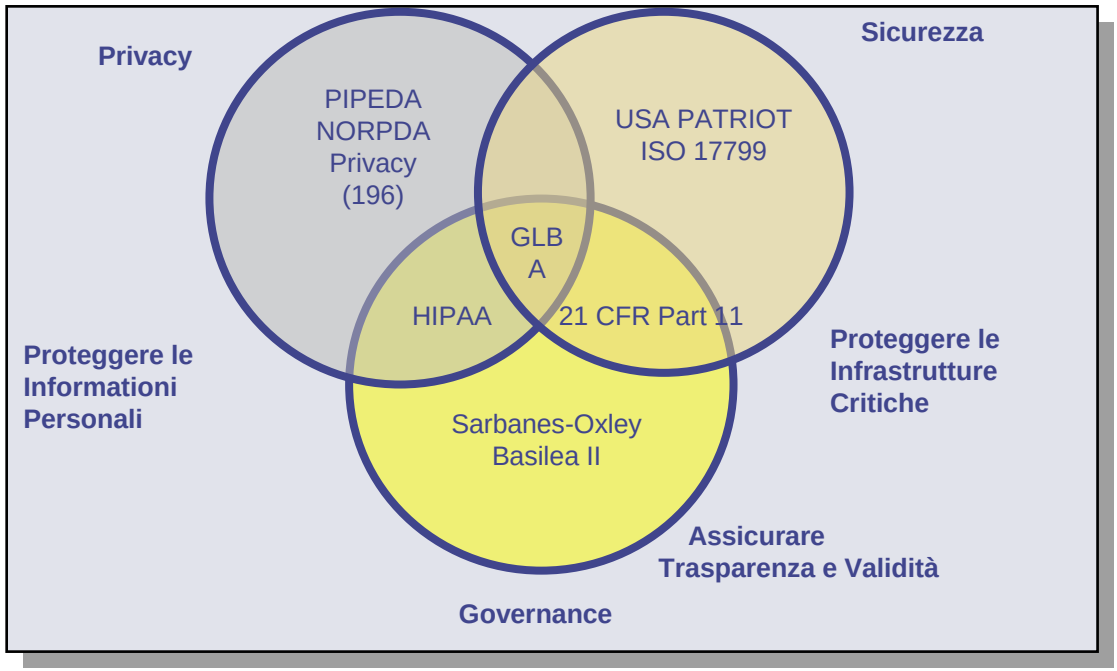


Figura 1: Il Triangolo di Identity, Security, Privacy

La Conformità come priorità

- Necessità di conformità a un nuovo contesto di regolamenti e normative internazionali e locali (D.Lgs 196/2003)
- I legislatori mirano alla 'qualità sostanziale' dei modelli di business aziendali e dei sistemi informativi che li supportano. Allineare il business all'IT per creare la "**Transparence Enterprise**"

Normative che convergono e impongono nuovi costi e nuovi processi per implementare la sicurezza sui dati, sugli accessi, sulle applicazioni sui modelli di business



Common Elements of all Regulations

The most common element of all regulations is a ***strong set of internal controls***. An internal control is a set of procedures that can ensure the successful operation of a business practice or transaction.

These controls must provide:

- **Accountability** – who performed an action, who approved it, when was it done, and what was the result?
- **Transparency** – all business processes and controls must be fully understood, and clearly documented. Opaque processes are, by definition, non-compliant.
- **Measurability** – All internal processes must be able to be measured and evaluated as to success or failure. Measurement is done through auditing, logging, correlation, and visualization.

Internal Control Frameworks

Regulations don't prescribe actual technologies to use for compliance. Instead, most companies adopt internal control frameworks as models of "best practice" for compliance. Some popular frameworks include:

- **COSO --** defines requirements for effective corporate governance.
- **CobiT –** defines IT governance and control practices.
- **ISO 17799 --** defines best practices in information security.
- **ITIL --** defines the processes and activities to support IT services

L'Importanza della Security per le Normative

Regulation Technology	SOX	HIPAA	Gramm -Leach Bliley	Sec 17A-4	21 CFR Part 11	Basel II	USA Patriot Act	CA SB 1386	Canada PIPEDA
Financial Compliance	✓								
Business Intelligence & Data Warehousing	✓								
Document / Content Management & Access	✓	✓	✓	✓	✓	✓	✓	✓	
Records Management	✓	✓	✓	✓	✓	✓			
Archiving	✓	✓	✓	✓	✓	✓	✓	✓	
Security	✓	✓	✓	✓	✓	✓	✓	✓	✓
Storage	✓	✓		✓	✓	✓	✓		

Top 10 IT-Related Design Control Deficiencies

#10 System documentation does not match actual process

#9 Inadequate documentation, identification and tracking of IT assets

#8 Custom programs, tables, & interfaces unsecured

#7 Posting periods not restricted within GL application

#6 Terminated employees or departed consultants still have access

#5 Large number of users with access to "super user" transactions in production

#4 Development staff can run business transactions in production

#3 Lack of "transparency" over changes made to Financial Applications

#2 Database (e.g. Oracle) and Operating system (e.g. Unix) supporting Financial Applications or Portal not hardened

#1 Unidentified or unresolved segregation of duties issues

* Ken Vander Wal, National Quality Leader, E&Y ISACA Sarbanes Conference, 4/6/04

7 of Top 10 Deficiencies are IAM-Related!!!

Example: CobiT DS5 & a Compliance Platform

DS5 (System Security) Reqs	Identity Mgt	Access Mgt	Provisioning	Monitoring
Manage Security Measures	✓	✓	✓	✓
Identification, Authentication, and Access	✓	✓	✓	
Security of Online Access to Data	✓	✓	✓	
User Account Management	✓		✓	
Management Review of User Accounts	✓	✓	✓	✓
User Control of User Accounts	✓		✓	✓
Security Surveillance		✓	✓	✓
Data Classification		✓		
Central Identification and Access Right Management	✓	✓	✓	
Violation and Security Activity Reports		✓	✓	✓
Incident Handling		✓		✓

Example: CobiT DS5 & a Compliance Platform (cont)

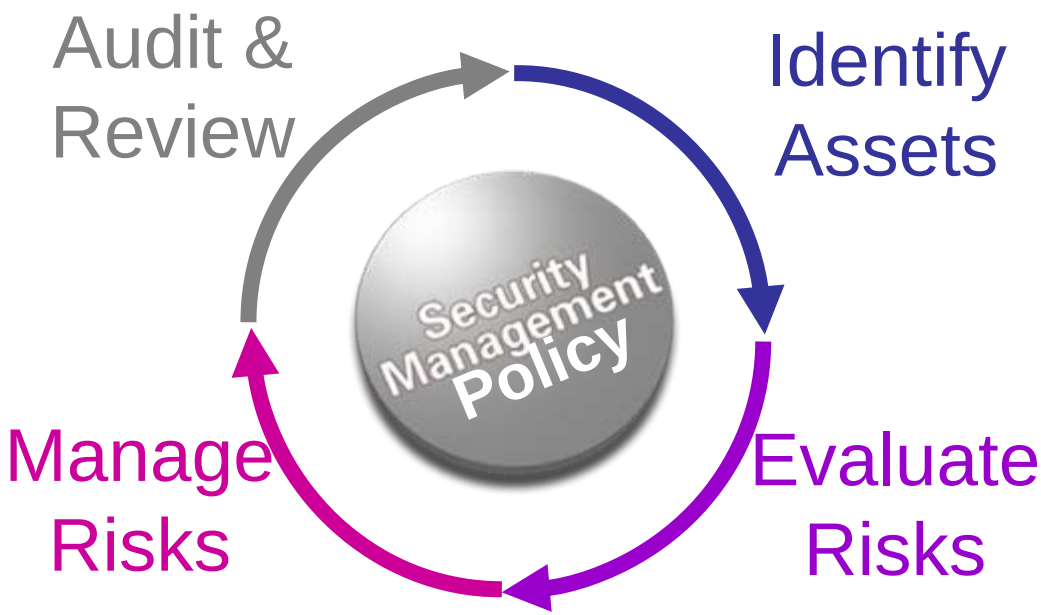
DS5 (System Security) Reqs	Identity Mgt	Access Mgt	Provisioning	Monitoring
Re-accreditation				
Counterpart Trust		✓		
Transaction Authorization		✓		
Non-repudiation		✓		
Trusted Path		✓		
Protection of Security Functions		✓		
Cryptographic Key Management		✓		✓
Malicious Software Protection, Detection, and Correction		✓		
Firewall Architectures and Connections with Public Networks				
Protection of Electronic Value				

not applicable to IAM

Conclusion: a comprehensive compliance platform can provide the technology to meet the needs of SOX section 404.

Information Security Management

ISO/IEC 17799 Code of Practice for Information Security Management.



Identity and Access Management

- ISO 27001
- EA-7/03
- CobiT

- Data
- Applications
- Transactions
- Web sites
- Directories

- Provisioning
- HR Integration
- Strong Authentication
- Single Sign-On
- Access Control
- Separation of duties
- Logging

- Personnel
- Credentials
- Multiple Sign-On
- Excess privilege
- Admin accounts
- Access rights creep
- Orphan accounts

BS7799 Controls

- **Security Policy** – management direction and support for information security.
- **Organisation of Assets and Resources** – to manage information security.
- **Asset Classification and Control** –identify assets and protect them.
- **Personnel Security** – reduce the risks of human error, theft, fraud, or misuse.
- **Physical and Environmental Security** – prevent unauthorised access, damage, and interference to business premises and information.
- **Communications and Operations Management** – ensure the correct and secure operation.
- **Access Control** – control access to information.
- **Systems Development and Maintenance** – ensure that security is built into information systems.
- **Business Continuity Management** –protect critical business processes from the effects of major failures or disasters.
- **Compliance** – avoid breaches of law, statutory, regulatory, and contractual obligations.

BS7799 Identity Considerations

- **General Controls**
  - Clear screen policy
- **Operations Management**
  - Segregation of duties
  - Operator logs
- **Electronic Commerce security**
  - Authentication
- **User access management**
  - User registration
  - Privilege management
  - User password management
  - Review of access rights
- **OS Access Control**
  - Terminal log-on procedure
  - User identification and authentication
  - Password management system
  - Use of system utilities
  - Terminal time-out
- **Application Access Control**
  - Information access restriction
  - Monitoring system access & use
- **Cryptography**
  - Non repudiation of digital sigs

D.L. 196/03 “Testo Unico sulla Privacy”
Art. 34 – Trattamenti con strumenti elettronici

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell’allegato B), le seguenti misure minime:

- a) **autenticazione** informatica;
- b) adozione di procedure di **gestione delle credenziali di autenticazione;**
- c) utilizzazione di un sistema di **autorizzazione**;
- d) aggiornamento periodico dell’individuazione dell’ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici

D.L. 196/03 "Testo Unico sulla Privacy" Allegato B: Disciplinare tecnico in materia di misure minime di sicurezza

- **Autenticazione Informatica**
- **Procedure di gestione delle credenziali di autenticazione**
- **Uso di un sistema di autorizzazione**

Il trattamento dei dati è consentito solo agli incaricati dotati di credenziali di autenticazione (codice identificativo + parola chiave riservata conosciuta solo dall'incaricato……) o strong authentication biometrica o a smart card e simili

Profili di autorizzazione per ciascun incaricato o per classi omogenee:

- criteri di individuazione preventiva
- verifiche periodiche (almeno ogni anno)
- criteri di revoca

Gestione dei codici identificativi:

- Criteri di definizione e assegnazione
- Individualità / non riusabilità
- validità temporale (disattivazione per mancato utilizzo – 6 mesi – o perdita qualità)

Gestione delle parole chiave (password):

- criteri di creazione (almeno 8 caratteri o massimo consentito dal sistema, non banale, ecc.)
- criteri di gestione (cambio ogni 6 mesi; 3 mesi se dati sensibili) e di custodia

Ad ogni incaricato possono essere associate una o più credenziali

Il titolare dovrà fornire agli incaricati precise istruzioni in merito:

- alla gestione e conservazione delle credenziali di autenticazione
- alla custodia dei dispositivi in possesso e uso esclusivo dell'incaricato
- alla gestione e custodia dello strumento elettronico durante le sessioni di trattamento
- individuazione puntuale delle modalità di accesso ai dati, in caso di assenza prolungata o impedimento dell'incaricato, per esigenze organizzative e di sicurezza aziendale

Dalla norma ai controlli

Troppo facile violare gli archivi ... senza lasciare tracce. Lo ha accertato il Garante della Privacy che impone ... controlli più rigidi

I tecnici del Garante, ...si sono resi conto che alcuni funzionari di alto livello, chiamati in gergo 'addetti IT' o anche amministratori di sistema ... potevano consultare ed estrarre dati ... senza lasciare tracce. L'apparato informatico, infatti, era congegnato in modo da segnalare il loro ingresso, ma non le operazioni compiute.

(Da un articolo di giornale....primavera 2006)

Provvedimento del Garante del 01/06/2006

1. **Tracciamento di tutte le operazioni sui dati o di attività che implicano autorizzazioni di accesso ai dati [Utenti, Applicazioni, System Admin, DBA] garantendone completezza, integrità e non ripudio (per "non ripudio del tracciamento di tutte le operazioni sui dati o di attività", si è intesa la non ripudiabilità delle registrazioni contenute nel log di tali operazioni).**

2. **Assicurare che i profili di autorizzazione dei data base administrator e dei system administrator siano effettivamente limitati ai dati e alle operazioni loro affidate e non comportino la capacità, anche potenziale, di trattare dati personali diversi da quelli necessari.**

3. **Assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.**

4. **Adottare procedure informatiche in grado di garantire la rigida separazione delle funzioni tecniche di assegnazione di credenziali di autenticazione, di privilegi di accesso ai dati e di autorizzazioni rispetto a quelle di gestione tecnica dei sistemi e delle basi di dati, escludendo che tali funzioni possano essere attribuite a uno stesso incaricato.**

Identity Management: Fasi e Funzioni

- Identificazione

  Riconoscimento del soggetto mediante una *credenziale* (o *identificativo*)

- Autenticazione

  Verifica della rispondenza dell'identità del soggetto

- Autorizzazione

  Accesso alle risorse richieste dal soggetto sulla base delle informazioni fornite nella fase di autenticazione

Identity Management: Fasi e Funzioni

- Auditing/Monitoring

  Le azioni dell'utente sono registrate nei log ed i log sono auditati, possono essere automatizzati degli eventi

- Single Sign-On

  Autenticazione centralizzata per l'accesso ai diversi sistemi ed applicazioni

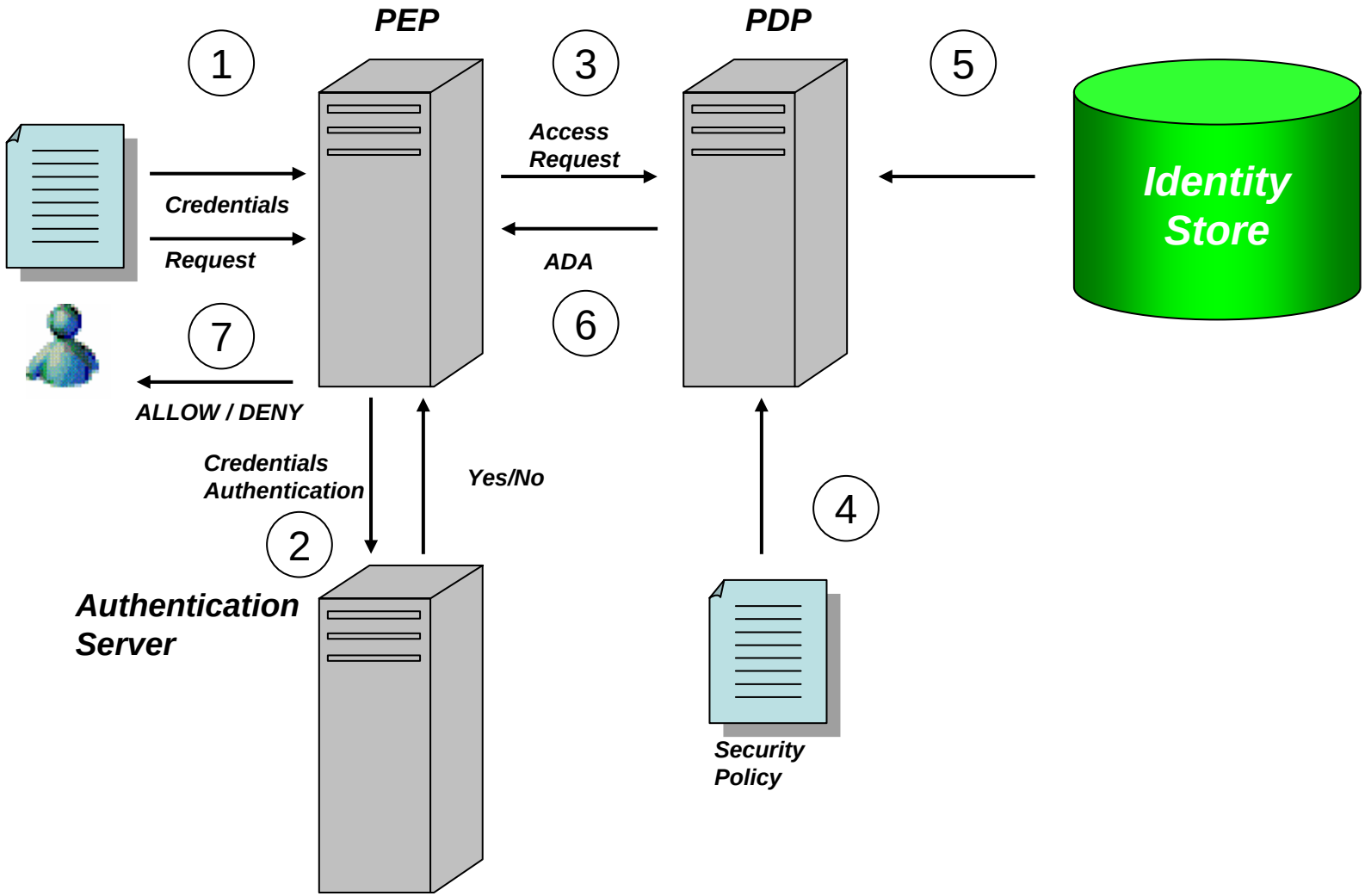
- Provisioning / De-provisioning

  Definizione / Rimozione degli *account* degli utenti e dei diritti di accesso alle risorse

- Workflow

  Processi di approvazione e notifica

Autenticazione e autorizzazione



Che cosa è l'Identity & Access Management

- L'Identity & Access Management è l'insieme dei processi e dell'infrastruttura che li supporta dedicati alla creazione, alla gestione e all'utilizzo delle "identità digitali" assieme all'applicazione (enforcement) delle policy organizzative e di business
- Raggiunge tali obiettivi rispondendo a:

Chi è? Cosa può fare?

- Identification and Authentication Management
- Access Control (Authorization Management)

Come viene gestito?

- User Management
- Delegated Administration
- Workflow

Di che cosa ha bisogno?

- Account Provisioning
- Account Deprovisioning

Identity Management

La piattaforma di Identity Management:

- È l'infrastruttura per centralizzare il controllo e l'auditing dell'accesso di tutti gli utenti alle risorse protette
- Centralizza la gestione del profilo identificativo degli utenti e dei loro diritti d'accesso
- È la soluzione per automatizzare la Conformità

IM: Il Processo

Clearly Define Identity Management Process and Responsibilities:

- Who defines access roles/privileges.
- Who decides who gets roles/access privileges.
- Who assigns roles/access privileges.
- Who approves changes.
- What are the End User responsibilities.
- From induction to termination.
- For employees, partners and customers

Piattaforma IAM

Employees
Associates
Contractors
Temps

Intranet

Customers
Partners
Supply chain

Internet

SAML
SPML
XACML

Partner
Identity
Federation
Provisioning
Applications

Help Desk

HR System

XML
SPML

Provisioning Administration
Policy, Role & group
Automation
Account
Workflow
Password
Delegation

Single Sign-on
Flexible
Authentication
RBAC
Legacy
Web Desktop
No change

Server Access Management
Role based access control
Administration - Separation of Duties
Server hardening

Extranet Access Management
Web authentication
Role based access control
Web single sign-on
User self-service

Policy Service
Who can access
What resource
In what way
From where
At what time

LDAP Directory
Employees
Contractors
Partners
Customers

Enterprise Infrastructure

Authentication Service
Username
Token
Certificate
Smartcard
Biometric

Physical
Badges
Building access
Zone access
Desk
Telephone
Mobile phone
PDA

IS Platforms
Windows Domain
Email
Mainframe
DBMS
Portal
Applications

IS Applications
CRM
ERP
SCM
SAP
Websphere
WebLogic
....

Auditing
Event logging
Event filtering
Notification
Storage
Searching
Reporting

Autenticazione

- **Metodi**
  - Basic Username / Password
  - Forms-based over SSL
  - Two factor tokens
  - Smart cards
  - X.509 certificates
    - Supporto completo CRL
    - Supporto OCSP
  - Sistemi Biometrici:
    - Fingerprint
    - Finger Scan
    - Voice print
    - Facial features
    - Hand Geometry
    - Iris Scan
    - Retinal Scan

Modelli di controllo accessi: DAC e MAC

- Discretionary Access Control
  - Il proprietario determina chi ha accesso e con quali privilegi.
- Mandatory Access Control
  - Basato sulle politiche organizzative aziendali
  - Proprietario e sistema determinano chi ha accesso.
  - Le decisioni di accesso sono basate sul privilegio (clearance) del soggetto e sulla sensitività (classification) dell'oggetto (es. file)
  - Richiede la classificazione con "label"
  - Inserisce le giuste limitazioni a coloro che stabiliscono le autorizzazioni.

Modello RBAC

"Un ruolo è una funzione lavorativa all'interno di un contesto organizzativo a cui vengono associate delle semantiche inerenti l'autorità e la responsabilità conferita all'utente a cui il ruolo viene assegnato."

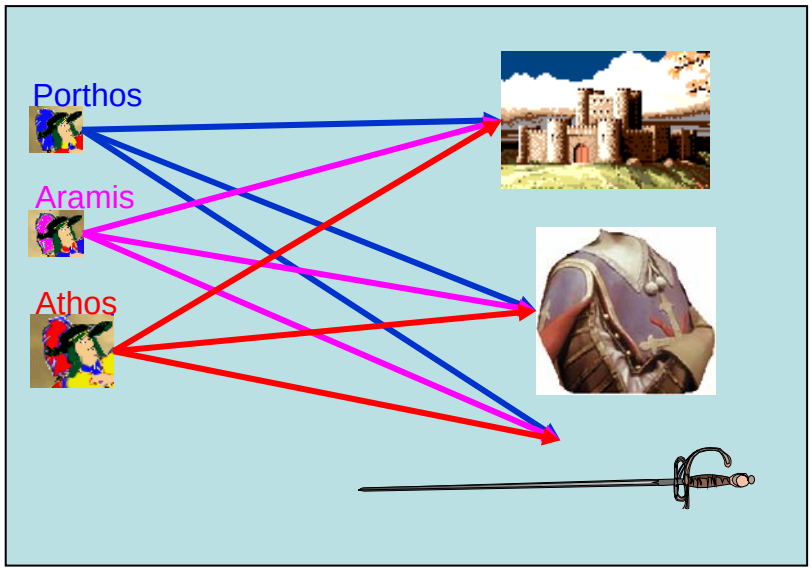
RBAC Standard from NIST

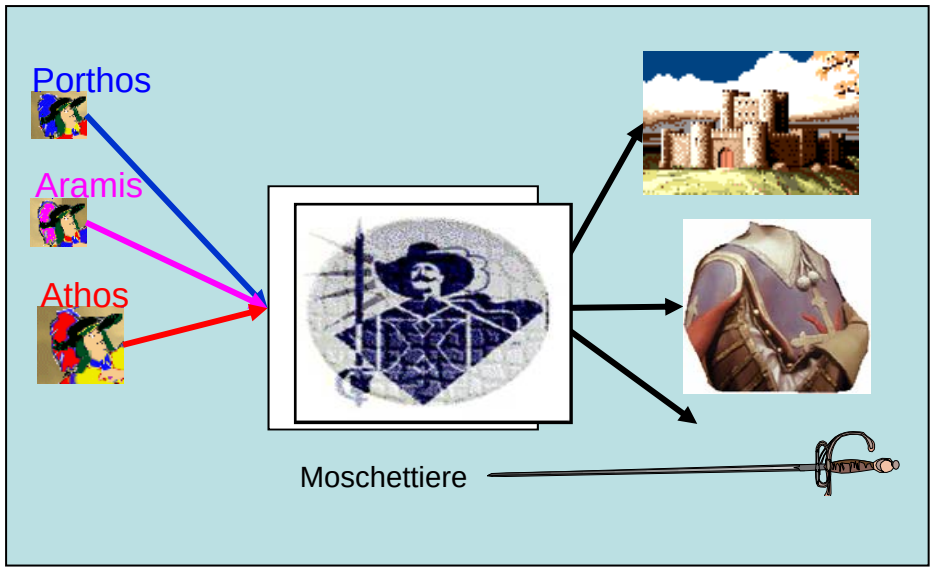
I ruoli sono essenziali per la scalabilità amministrativa in quanto:

- *Costituiscono un livello di astrazione che elimina le complessità*
- *I ruoli possono essere delegati*

Identity Management

"…processo che assegna risorse fisiche, logiche e servizi a dipendenti, business partner e clienti in base ai loro requisiti di business…"





IM come piattaforma di Conformità

Caratteristiche di una Piattaforma di Conformità

Principali funzionalità di IM e SIM:

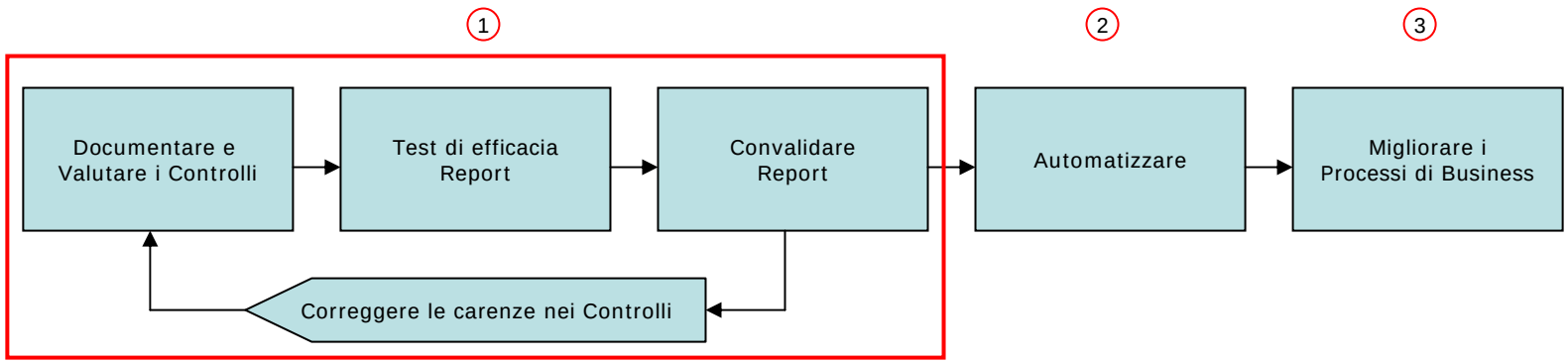
- Gestione centralizzata delle Identità e dei Diritti di Accesso degli utenti, tra tutte gli ambienti,
- Gestione automatizzata dell'accesso alle risorse a tutti gli utenti, basato sul "ruolo",
- Gestione automatizzata delle Identità degli utenti
- Prevenzione delle violazioni di "segregation of duties"
- Concessione dei minimi diritti di accesso richiesti per tutti gli utenti ("need to know")
- Monitoraggio dinamico dell'ambiente mediante auditing sicuri e report
- Risposta rapida ad eventi anomali o sospetti
- Rimozione automatica dei diritti d'accesso e delle Identità inutilizzate o scadute.
- Centralizzazione in tempo reale di collezionamento, reporting, filtraggio e correlazione di eventi di controllo accessi da network, sistemi ed applicazioni.
- Riduzione del rischio attraverso strumenti automatici di Vulnerability Assessment
- Rilevazione di incidenti di sicurezza attraverso strumenti di investigazione forense per auditing in profondità, visualizzazione ed analisi.

Il Processo di Conformità

Muoversi dall'Analisi di Conformità al miglioramento dei processi di business

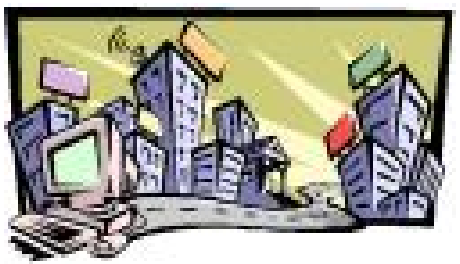
Si può schematizzare il Processo di Conformità in tre fasi:

1. Recepire i requisiti iniziali di Conformità
2. Creare una Struttura di Controlli Interni automatica e ragionevole
3. Migliorare i processi di business



Identity Federation

From policy point of view (trust)

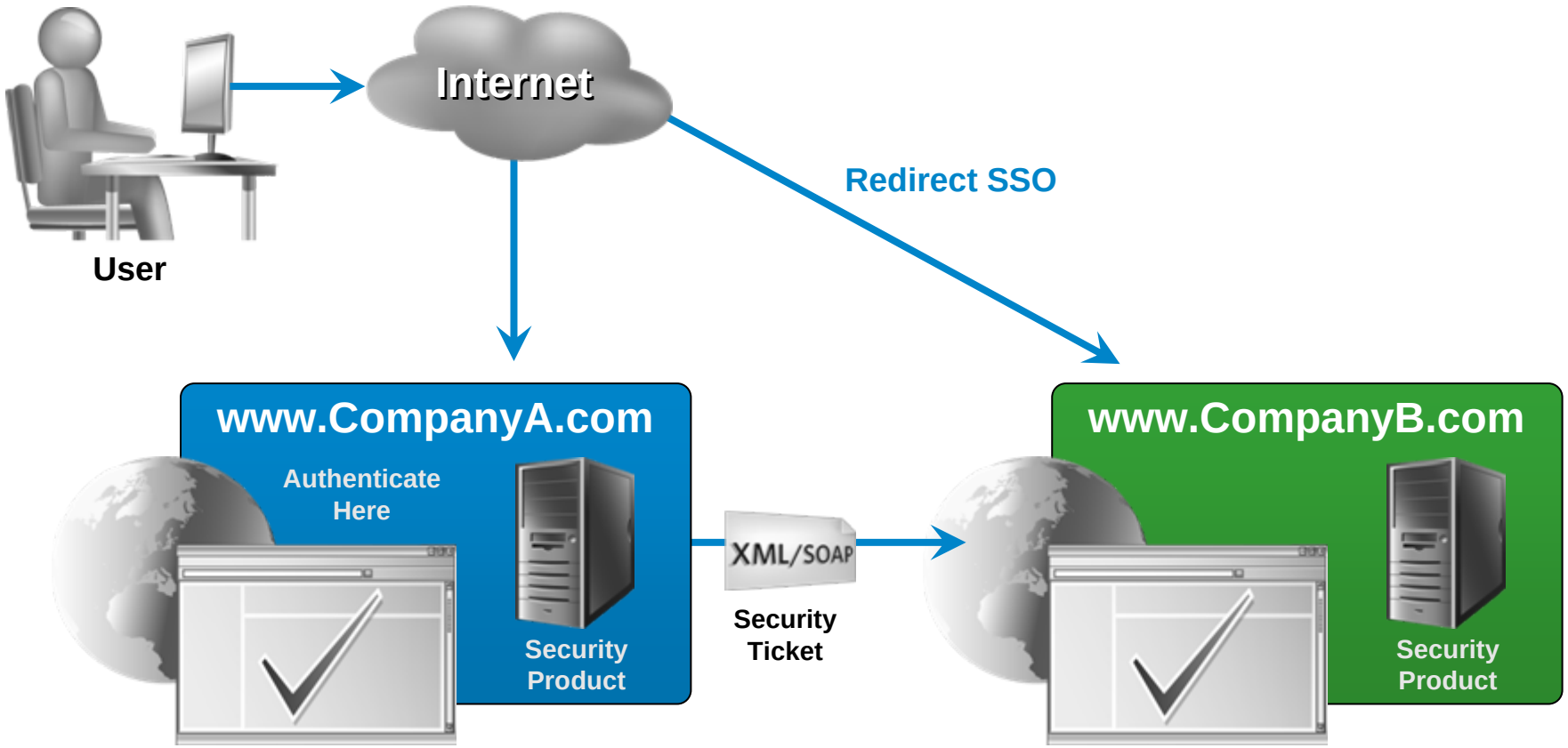


From technical point of view (communications)

L'Identity Federation si può definire come l'infrastruttura tecnologica, organizzativa e procedurale che permette ad un insieme di enti erogatori di servizi (es. i service provider) in relazione di fiducia (circle of trust), di condividere gli identificativi utente in modo sicuro. L'Identity Federation si realizza mettendo in collegamento sicuro i diversi identificativi, utilizzati dai differenti provider, relativi ad uno stesso utente reale. Praticamente, l'Identity Federation permette una trasmissione sicura di identità tra domini autonomi o più aziende.

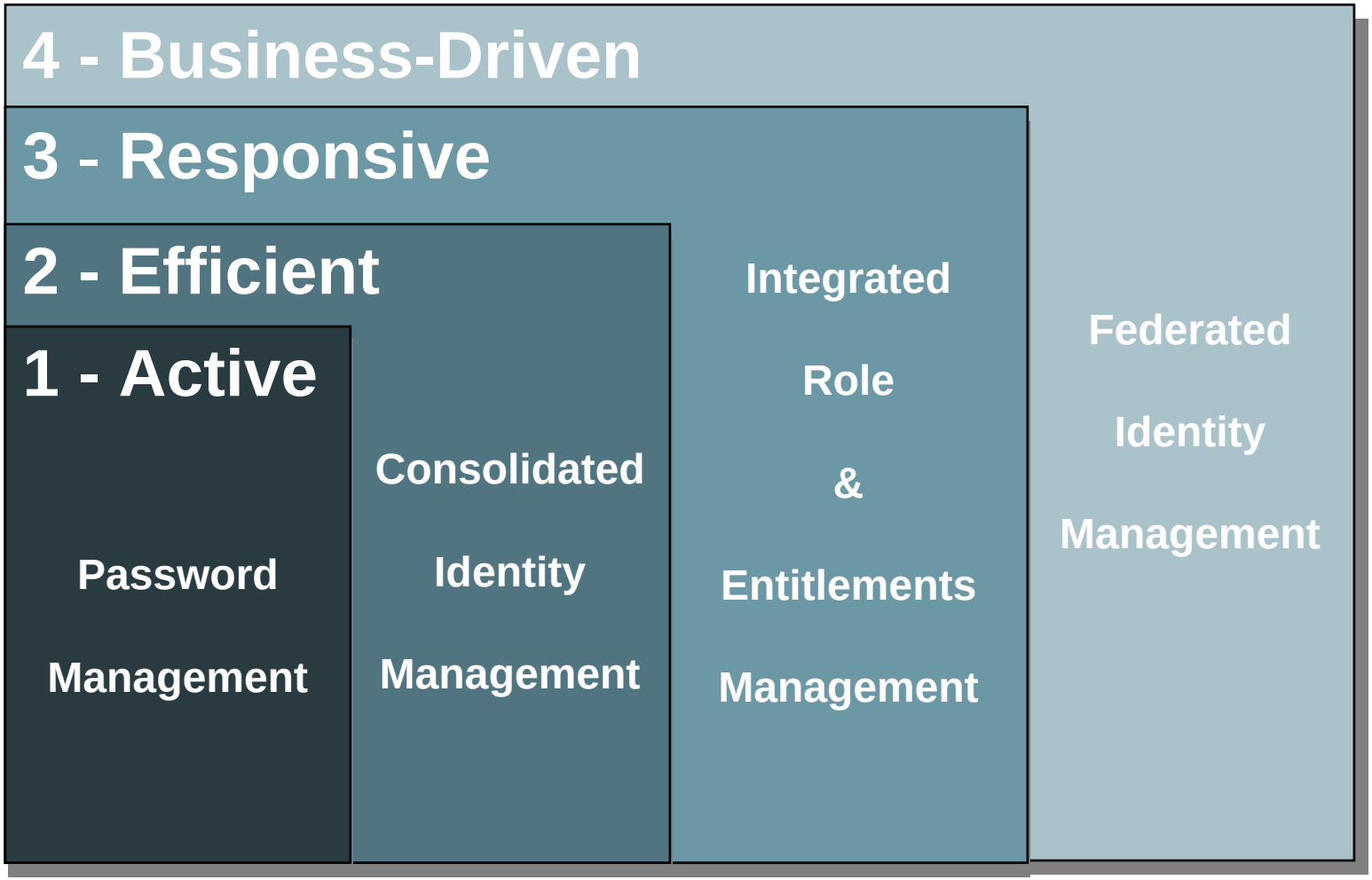
From business point of view (relationships)

Identity Federation



Protocolli per il federation: SAML, Liberty Alliance, WS Federation

Identity Management Maturity Model



Riferimenti

- Philip J. Windley – Digital Identity - O'Reilly Ed.
- Information Systems Control Journal
  - Articoli di Steven J. Ross: Vol. 3 – 2003, Vol. 4 – 2003
    Bill McQuaide: Vol. 3 – 2003
    Srinivasan Vanamali: Vol. 4 – 2004
    Leslie Pang: Vol. 4 – 2005
- ISO/IEC 17799 Code of Practice for Information Security Management
- COBIT 4.0
- Codice in materia di protezione dei dati personali - Decreto Legislativo 30 giugno 2003, n. 196

Domande?