GDPR & Governo delle Identità ed Autorizzazioni

Giacomo Parravicini

Identity & Security Area Manager

Giacomo.Parravicini@netstudio.it

IDENTITY GOVERNANCE – PANORAMICA

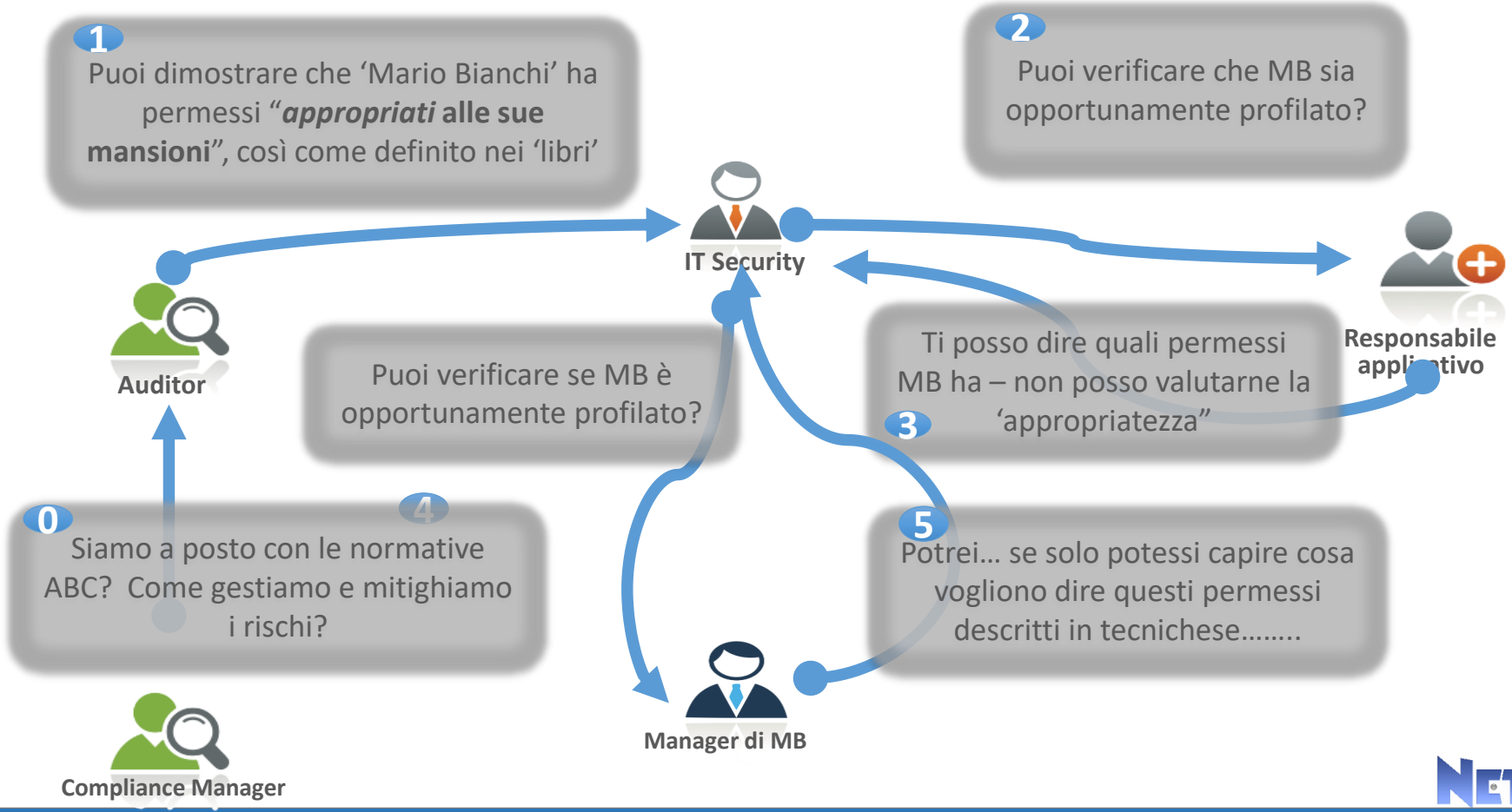
- L'identity Governance è l'insieme delle procedure, delle policy e dei controlli che consentono una corretta gestione dei diritti di accesso ad applicazioni strutturate e non.

- L'obiettivo principale dell'**Identity Governance** è consentire l'applicazione delle regole definite in merito a:
  - Processi relativi al ciclo di vita delle Identità
  - Processi di richiesta e revisione delle abilitazioni
  - Identificazione dei rischi di Separation of Duty ed altro

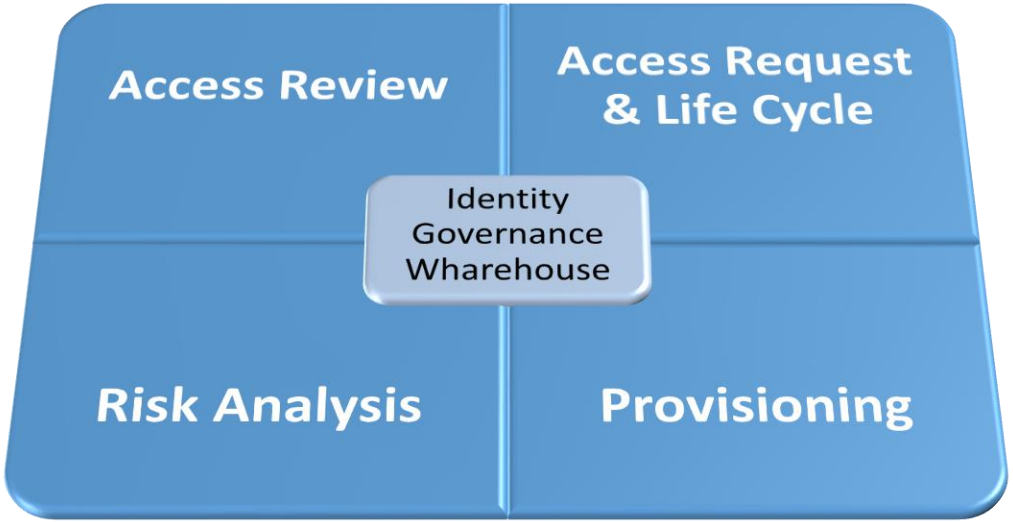
- IGA offre **strumenti di controllo e di mitigazione dei rischi** correlati all'assegnazione agli utenti delle autorizzazioni

- **Controllo e Mitigazione del Rischio** sono le parole chiave di riferimento di questa disciplina

LE DOMANDE A CUI RISPONDIAMO



IDENTITY GOVERNANCE FRAMEWORK



IDENTITY GOVERNANCE – PANORAMICA

Chi si occupa di **Identity Governance** deve essere in grado di dare risposta alle seguenti domande:

- Sto adeguatamente tutelando *(valutazione del rischio)* l'accesso alle informazioni ed i dati sensibili?
- Sono in grado di identificare potenziali accessi ***non autorizzati*** alle informazioni?
- Sono in grado di ***certificare*** gli accessi e garantire a riguardo dell'accuratezza delle ***revoche***?
- Posso provare la ***conformità*** alle normative?

IDENTITY GOVERNANCE – REQUISITI DI BASE

I requisiti funzionali di un progetto di Identity Governance sono:

- Aderenza al principio del ***«Minimo Privilegio»***
- Assegnazione abilitazioni attraverso procedure di richiesta coerenti, ripetibili e tracciabili e non per ***«copia account»***
- Disattivazione o cancellazione degli account in coerenza al ***ciclo di vita dell'identità***
- Rilevazione di utenti che, attraverso gli accessi concessi, possono svolgere attività in conflitto tra loro (***Sepatation of Duty***)
- Revisione periodica delle abilitazioni
- Controllo e limitazione della presenza di account orfani, applicativi e di servizi

IDENTITY GOVERNANCE – CRITICITA IN MERITO AI DATI

Per governare occorre conoscere:

- Non esiste una visione unica e complessiva (***su tutte le applicazioni***), sempre consultabile, delle identità e delle autorizzazioni rilasciate ("***chi" fa "cosa"***)
- Molto spesso i profili presenti sui sistemi non sono conosciuti e/o non parlanti e la verifica risulta di difficile attuazione da parte di un responsabile di ufficio.
- Non esiste un modello di riferimento per la progettazione del catalogo delle autorizzazioni

IDENTITY GOVERNANCE – CRITICITA IN MERITO AI PROCESSI

Diritti di accesso "eccessivi" rispetto agli effettivi compiti aziendali:

- Le logiche di richiesta di risorse applicative sono spesso eseguite sotto il profilo della necessità funzionale ed operativa e quasi mai sotto una logica di sicurezza.

- Le richieste di autorizzazioni sono effettuate tramite moduli di richiesta indicando un utente di riferimento da cui copiare le abilitazioni.

- Le abilitazioni di accesso aumentano sempre al variare degli incarichi delle persone. ***(meglio qualcosa il più che qualcosa in meno !)***

IDENTITY GOVERNANCE – CRITICITA IN MERITO AI CONTROLLI

L'analisi dei conflitti SoD costituisce uno dei controlli principali di compliance.

- Non esiste un modello logico che, a partire dai processi aziendali, identifichi le "attività incompatibili" all'interno di ciascun processo e tra processi differenti
- Non esiste una mappatura delle attività dei processi (specialmente quelle incompatibili) nelle applicazioni/profili che permettono di "esercitarle"
- Di conseguenza, non esistono realmente dei controlli preventivi di segregazione effettuati nel momento in cui si fa una richiesta o come analisi periodica delle abilitazioni presenti in un sistema

IDENTITY GOVERNANCE – OBIETTIVI

Gli obiettivi che generalmente devono essere raggiunti sono:

- Garantire che ciascun utente disponga, in ogni momento, di tutte e solo le abilitazioni di accesso necessarie a svolgere il proprio lavoro, riducendo il rischio di accesso illecito a dati ***(privilegio minimo).***

- ***Rendere tracciabili le richieste di accesso*** in termini di chi e quando ha effettuato la richiesta, cosa è stato chiesto, chi ha approvato e chi è stato abilitato.

- ***Rendere facilmente visibili/comprensibili/revisionabili le abilitazioni*** assegnate sull'intero parco applicativo.

- Definire e implementare un modello SoD.

- ***Rendere il processo di richiesta da «inconsapevole»*** (basato su principi di cui non si ha conoscenza) ***a «consapevole» e «responsabile»*** (basato su cataloghi strutturati e comprensibili).

IDENTITY GOVERNANCE – METODOLOGIA PROGETTUALE

- Identities Collection
- Accounts Collection
- Permissions & Assignments Collection
- Identify Unmatched Accounts
- Correlate Identities & Accounts
- Automatic Provisioning

Integration

- Design Access Request
- Design Access Review
- Life Cycle Processes
- Permission Translation & Classification
- Role design / Mining
- SoD & Others Policy Design

Design

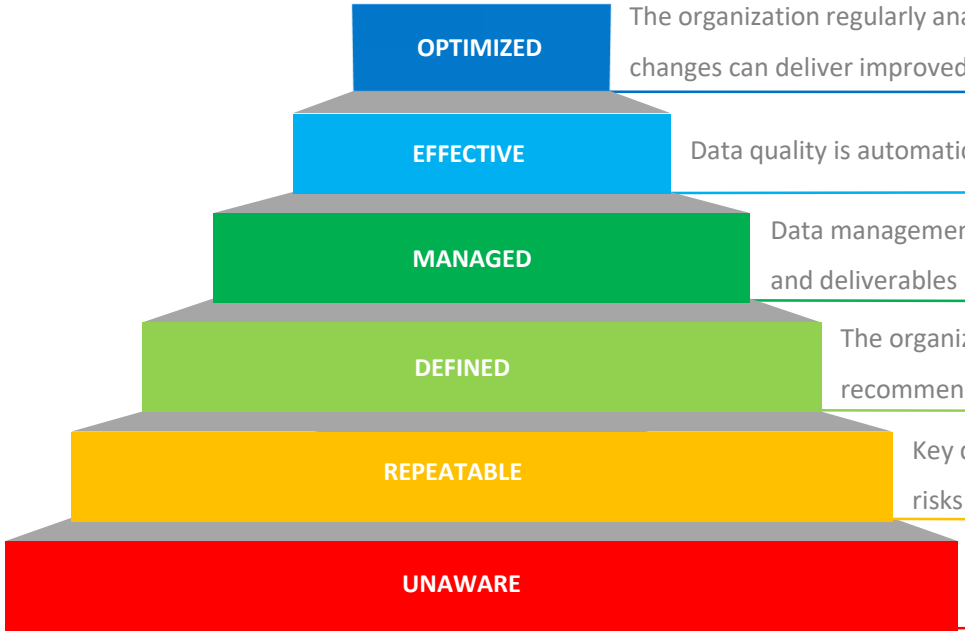
- SoD User & Role Check
- Out of band Assignment
- In band Assignment not completed
- Orphan / Dormant Accounts
- Preventive SoD Check

Control

- Mitigation Control
- Report & Notify
- Period Role & User review
- Access request Form

Mitigation

DATA QUALITY -MODEL



The organization regularly analyses existing data management processes to determine where changes can deliver improved efficiencies

Data quality is automatically monitored and reported

Data management processes are required and monitored. They are a core part of projects and deliverables

The organization uses a set of defined rules and processes that are published for recommended use

Key data management individuals are assigned to critical projects to reduce risks and improve performances by replicating best practices

Data management is characterized as ad hoc. There is no awareness of data management practices; results are variable and unrepeatable

COBIT PROCESSES MATURITY MODEL

QUALITY COVERAGE

- Identities Collection
- Accounts Collection
- Permissions & Assignments Collection
- Identify Unmatched Accounts
- Correlate Identities & Accounts
- Automatic Provisioning

Integration

- Design Access Request
- Design Access Review
- Life Cycle Processes
- Permission Translation & Classification
- Role design / Mining
- SoD & Others Policy Design

Design

- SoD User & Role Check
- Out of band Assignment
- In band Assignment not completed
- Orphan / Dormant Accounts
- Preventive SoD Check

Control

- Mitigation Control
- Report & Notify
- Period Role & User review
- Access request Form

Mitigation

IDENTITY GOVERNANCE – PERCORSI DI PROGETTO

Un'organizzazione che avvia un progetto di Identity Governance ***è consapevole che***, per raggiungere i propri scopi, dovrà cambiare i processi e le tecnologia fino a quel momento adottati.

- Da dove si parte ?
- Su quali aspetti mi devo concentrare ?
- Cosa hanno fatto le altre aziende per avere successo ?

IDENTITY GOVERNANCE – PERCORSI DI PROGETTO

In tanti anni di progetti abbiamo imparato molte lezioni su come pianificare, staffare e realizzare un progetto di Identity Governance, come evitare errori comuni e passi falsi.

- Un progetto non è una questione solo di tecnologia
- Per il suo successo occorre:
  - Coivolgere le persone, rivedere processi ed implementare la tecnologia.
  - Definire precisamente obiettivi e metriche di misura del loro raggiungimento
  - Staffare persone chiave, a tutti i livelli, nel team di progetto (non solo risorse IT)

I progetti falliscono per:

- Incapacità di dimostrare chiaramente i risultati di business raggiunti.
- Complessità di progetto.

IDENTITY GOVERNANCE – SUGGERIMENTI

1. Partire con una chiara definizione delle esigenze di business

   - Il primo passo non è l'RFP per la selezione software ma bensi una valutazione (assessment) della situazione corrente.
   - Il risultato quindi non è il nome della tecnologia da utilizzare ma bensi una chiara comprensione della propria situazione e dei propri obiettivi, L'elenco dei processi e delle policy da migliorare, i propri punti di forza e di debolezza.

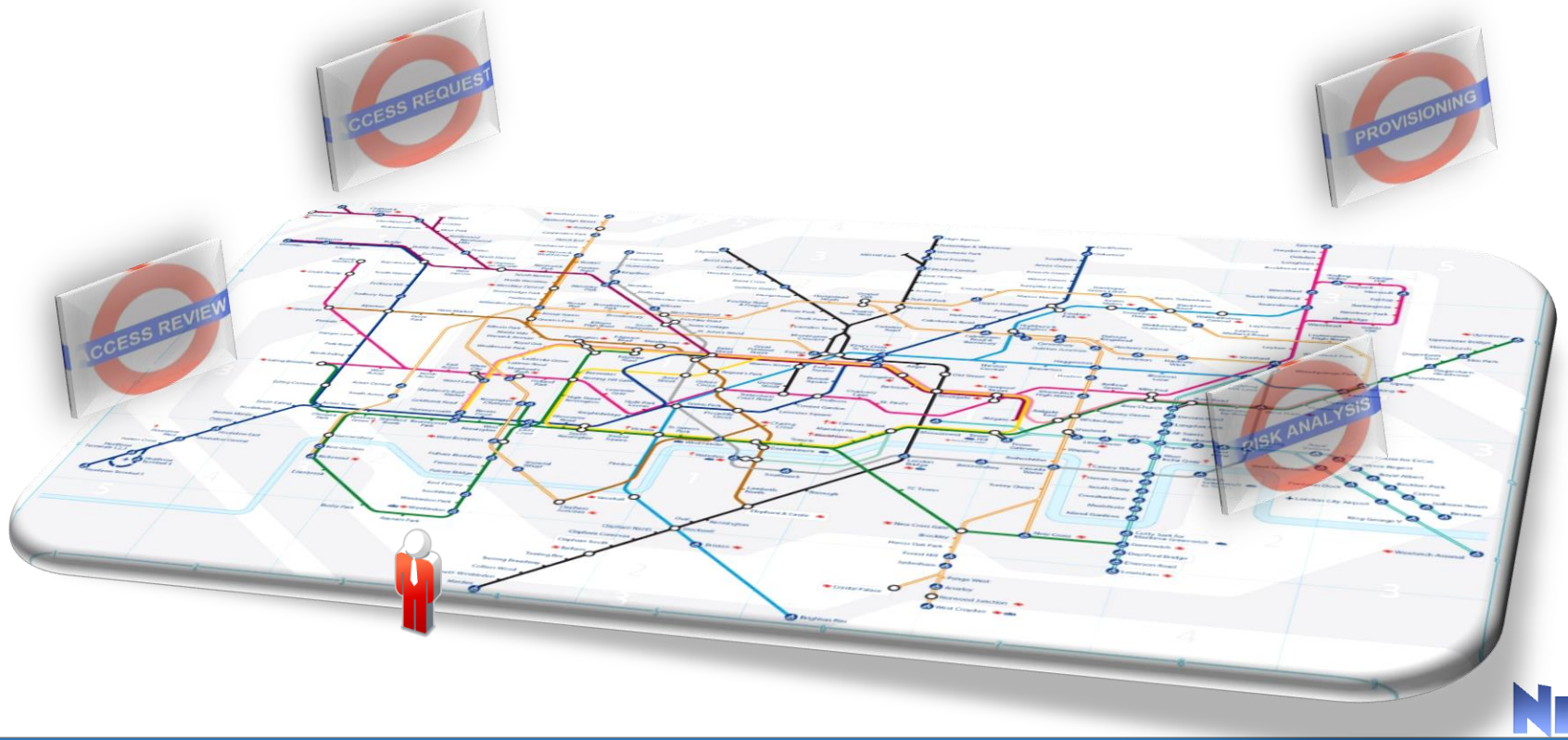
2. Coinvolgere le persone giuste

3. L'ownership e la responsabilità dei rischi deve essere ri-assegnato alle persone giuste.

4. Comunicare i risultati preventivamente e spesso

5. Evitare un approccio a «Big Bang»

IDENTITY GOVERNANCE – PERCORSI DI PROGETTO



IDENTITY GOVERNANCE – FASE 1 – REVISIONE ACCESSI

- Identity Collection
- Account Collection
- Permission & Assignment Collection
- Identify Unmatched Account
- Correlate Identity & account
- Automatic Provisioning

Integration

- Design Access Request
- Design Access Review
- Life Cycle Process
- Permission Translation & Classification
- Role design / Mining
- SoD & Other Policy Design

Design

- SoD User & Role Check
- Out of band Assignment
- In band Assignment not completed
- Orphan / Dormant Account
- Preventive SoD Check

Control

- Mitigation Control
- Report & Notify
- Period Role & User review
- Access request Form

Mitigation

IDENTITY GOVERNANCE – FASE 2 – LIFECYCLE E RICHIESTE ACCESSI

- Identity Collection
- Account Collection
- Permission & Assignment Collection
- Identify Unmatched Account
- Correlate Identity & account
- Automatic Provisioning

Integration

- Design Access Request
- Design Access Review
- Life Cycle Process
- Permission Translation & Classification
- Role design / Mining
- SoD & Other Policy Design

Design

- SoD User & Role Check
- Out of band Assignment
- In band Assignment not completed
- Orphan / Dormant Account
- Preventive SoD Check

Control

- Mitigation Control
- Report & Notify
- Period Role & User review
- Access request Form

Mitigation

IDENTITY GOVERNANCE – FASE 3 – CONTROLLI SOD

- Identity Collection
- Account Collection
- Permission & Assignment Collection
- Identify Unmatched Account
- Correlate Identity & account
- Automatic Provisioning

Integration

- Design Access Request
- Design Access Review
- Life Cycle Process
- Permission Translation & Classification
- Role design / Mining
- SoD & Other Policy Design

Design

- SoD User & Role Check
- Out of band Assignment
- In band Assignment not completed
- Orphan / Dormant Account
- Preventive SoD Check

Control

- Mitigation Control
- Report & Notify
- Period Role & User review
- Access request Form

Mitigation