LA GESTIONE DELLA SICUREZZA CON
IBM Security Identity Governance

Premier Business Partner IBM™

ENGINEERING

IDENTITY & ACCESS MANAGEMENT

L'approccio Engineering ai progetti

- Fa parte del contesto più ampio delle tematiche legate alla sicurezza (secure content, secure access, secure business)
- "... è un set di soluzioni utilizzate per l'identificazione di utenti in un sistema e per controllare il loro accesso alle risorse all'interno di quel sistema associando diritti e restrizioni ad una sola identità riconosciuta "(fonte IDC)
- consente di:

– migliorare la capacità di rispondere alle necessità normative
– migliorare la sicurezza complessiva del sistema
– standardizzare i meccanismi di sicurezza
– ridurre i costi relativi alla gestione del processo
– agevolare e semplificare l'accesso al portafoglio applicativo

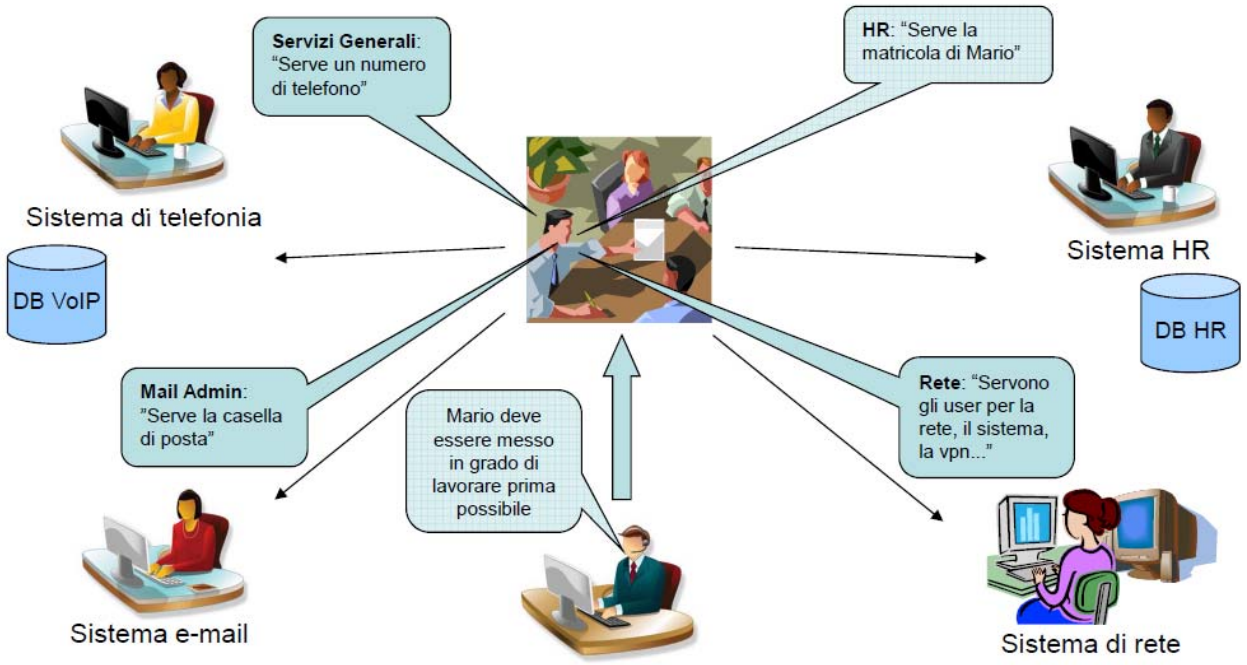
Premier Business Partner IBM

ENGINEERING

IDENTITY & ACCESS MANAGEMENT

L'approccio Engineering ai progetti

Hanno assunto Mario…



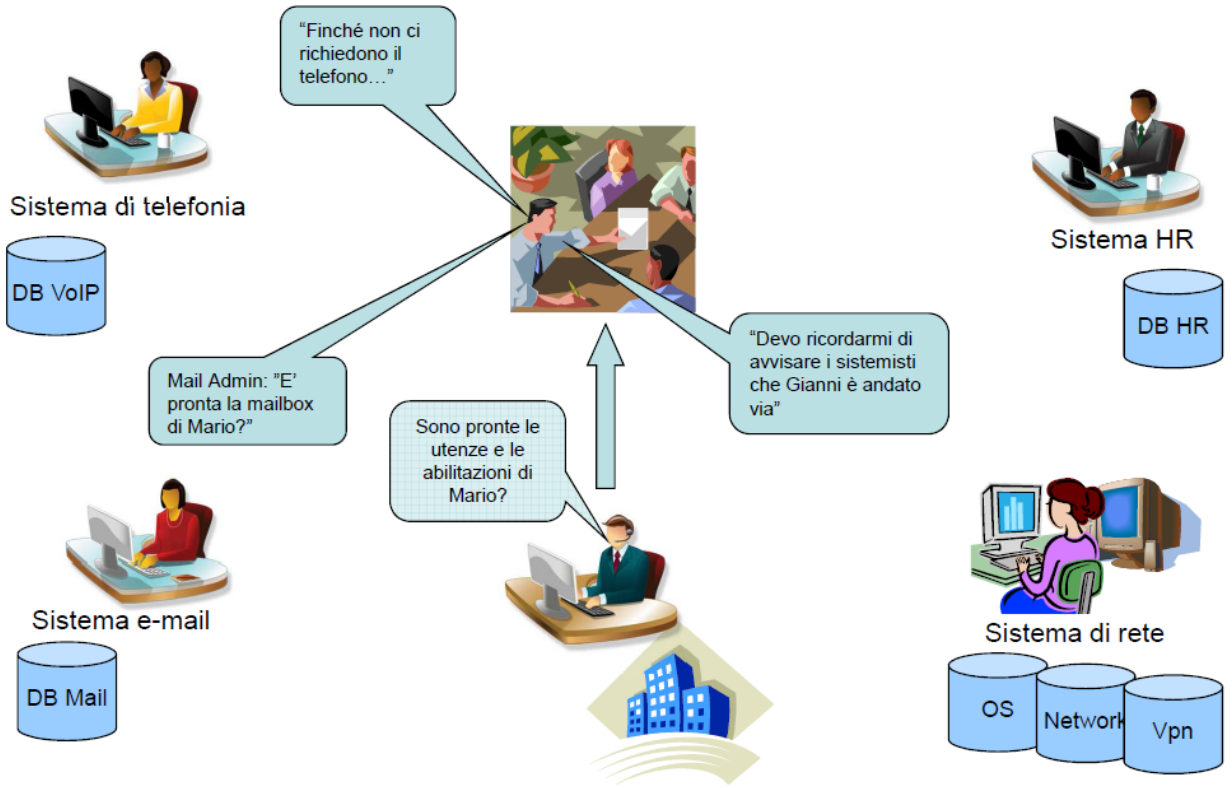
Premier Business Partner

ENGINEERING

IDENTITY & ACCESS MANAGEMENT

L'approccio Engineering ai progetti

Gianni ha dato le dimissioni…



IDENTITY & ACCESS MANAGEMENT

L'approccio Engineering ai progetti

Il CIO del Cliente…

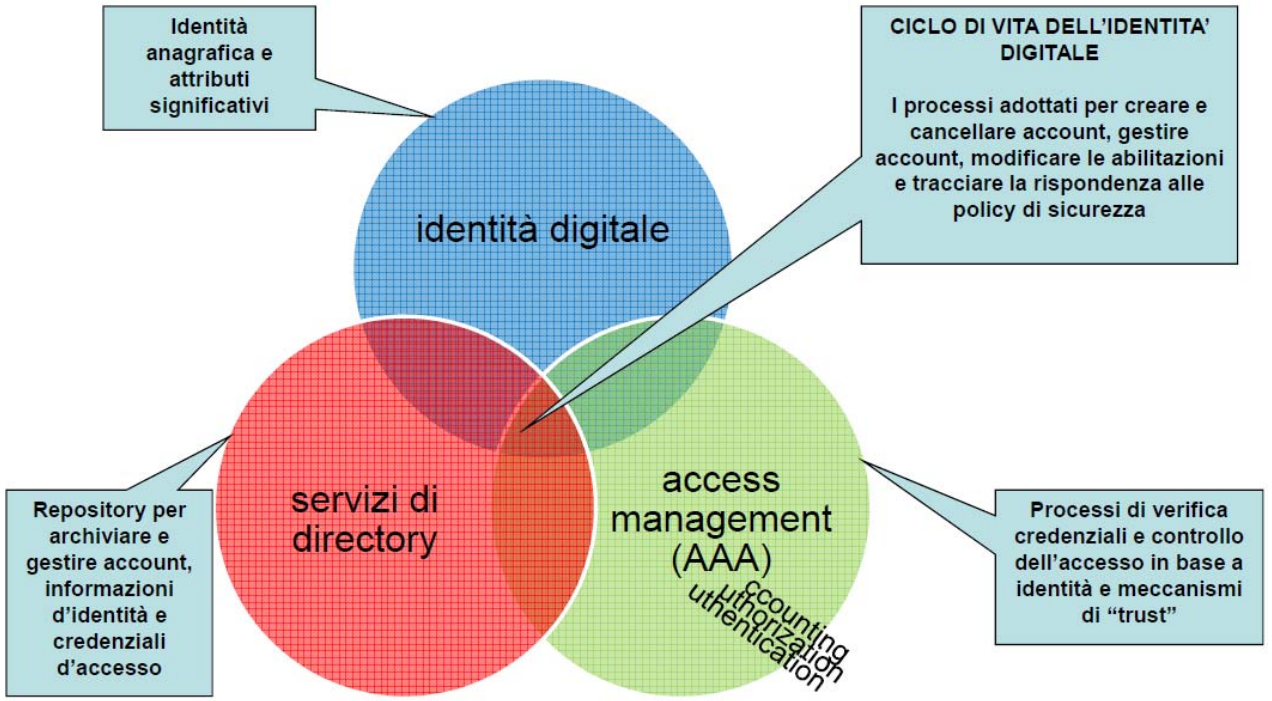
Quanto ci costa il processo?

- Quanto tempo ci vorrà perché Mario possa essere operativo?
- Come assicurare il provisioning corretto e coerente su tutti i sistemi?
- Chi approverà le modifiche agli accessi ed al profilo di Mario?
- Chi effettuerà l'audit sulla correttezza delle modifiche?
- Di quanti user-id e pwd avrà bisogno Mario?
- Avranno rimosso gli account di Gianni?
- Avranno recuperato il telefono di Gianni?
- …e se Gianni riceve mail dai fornitori?
- …

IDENTITY & ACCESS MANAGEMENT

L'approccio Engineering ai progetti

Elementi chiave



IDENTITY & ACCESS MANAGEMENT

L'approccio Engineering ai progetti

Definire l'identità digitale

Cosa contiene e quali sono l'identificativo principale e gli attributi d'interesse?

- Informazioni anagrafiche
  - cognome, nome, indirizzo, telefono, e-mail, codice fiscale, …
- Informazioni organizzative
  - ente di appartenenza, struttura organizzativa, matricola, sede, …
- Risorse assegnate
  - PC, Indirizzi IP, applicazioni, asset, ...

IDENTITY & ACCESS MANAGEMENT

L'approccio Engineering ai progetti

Attributi dell'identità digitale

Da chi e dove vengono gestiti gli attributi da trattare?

Quali sistemi informativi e quali strutture organizzative dispongono dell'informazione attendibile?

- chi sono i referenti interni
- quali sistemi dispongono dei dati master (MDM)
- quali strutture necessitano dell'informazione
- verso quali repository i dati devono essere replicati

...

Fondamentali per abilitare l'autorizzazione basata sugli attributi

IDENTITY & ACCESS MANAGEMENT

L'approccio Engineering ai progetti

Processi

Evidenziare processi e flussi

Identificare chi sono gli attori e quali sono le modalità di gestione dell'informazione

- come vengono gestiti i dati
- chi li manipola
- chi effettua il primo inserimento
- chi scatena le modifiche
- chi inserisce le variazioni
- quali sono le modalità di fruizione
- come possono essere gestite le deleghe

IDENTITY & ACCESS MANAGEMENT

L'approccio Engineering ai progetti

Governance

Identificare gli ambiti di utilizzo delle informazioni

Come si pensa di utilizzare le informazioni contenute nel sistema IAM

- viste che si vogliono ottenere
- accounting delle risorse impiegate
- reportistica relativa ai picchi di utilizzo
- attività di audit

IDENTITY & ACCESS MANAGEMENT

La Metodologia Engineering

APPROCCIO PROGETTUALE

La prima fase del progetto di implementazione riguarda la definizione (analisi e valutazione) dell'attuale modello di funzionamento della gestione degli accessi e della identità digitale del Cliente. Vengono raccolte tutte le informazioni necessarie per la comprensione dell'attuale gestione e per la predisposizione del nuovo modello a tendere.

In questa fase inoltre vengono svolte tutte le attività necessarie al dimensionamento del servizio e alla relativa attivazione. Vengono di seguito elencate le principali attività svolte nella definizione del progetto esecutivo che tenga conto delle effettive necessità operativo/funzionali del Cliente e che garantisca l'implementazione e l'attivazione dei nuovi servizi garantendo la continuità di quelli già in essere.

IDENTITY & ACCESS MANAGEMENT

La Metodologia Engineering

ASSESSMENT

Engineering utilizza un approccio che prevede un'attività di Assessment finalizzata a comprendere il contesto di business dell'Amministrazione e ad esaminare l'infrastruttura organizzativa pre-esistente.

Lo studio della situazione corrente ha l'obiettivo di pervenire alla descrizione del modello TO-BE da implementare, integrando e valorizzando le indicazioni emerse e le soluzioni già in uso.

Le attività di assessment specifiche per il progetto IAG sono basate su un insieme di interventi volti ad acquisire i dati necessari a conoscere e comprendere lo scenario dell'Amministrazione; tali attività consistono nell'analisi e rilevazione da effettuarsi su materiale disponibile direttamente nell'Amministrazione, mediante interviste differenziate in funzione del ruolo aziendale ricoperto, e tramite la compilazione di questionari o checklists predefiniti.

IDENTITY & ACCESS MANAGEMENT

La Metodologia Engineering

IMPLEMENTAZIONE

Baseline

L'architettura tecnologica viene implementata in tutte le sue componenti presso il Cliente sull'ambiente di Test. La stessa architettura viene replicata presso Engineering fungendo da ambiente di sviluppo.

Implementazione CORE

Implementazione Workflow

Implementazione Report

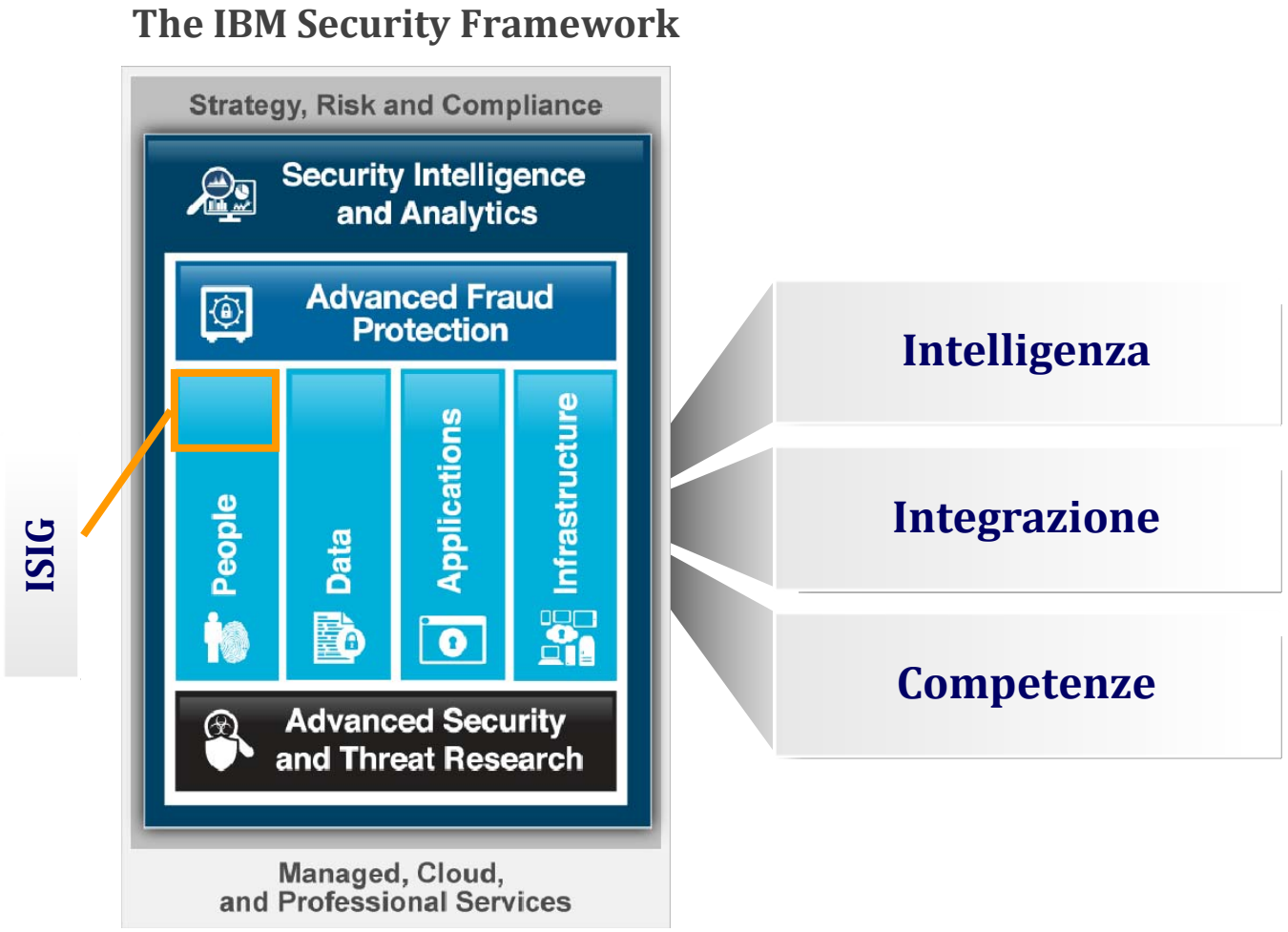
Implementazione connettori verso i sistemi target

Implementazione soluzione di SSO

Formazione

ISIG - IBM Security Identity Governance

Compliance, Audit e Controllo rischio accessi



Premier Business Partner

ENGINEERING

ISIG - IBM Security Identity Governance

Compliance, Audit e Controllo rischio accessi

Permette alle organizzazioni:

- la copertura completa ed efficace dei processi di gestione delle identità digitali relative agli utenti dei sistemi informatici nel rispetto delle procedure aziendali e dei vincoli di conformità rispetto a riferimenti normativi
- di ridurre i rischi di accesso, di frodi, di conflitti di interesse e di violazioni SOD.
- di evitare accessi non autorizzati ai dati e alle applicazioni da parte di utenti non in possesso dei necessari requisiti.
- di fornire agli utenti gli esatti permessi richiesti per l'esecuzione del loro lavoro: nulla di più e nulla di meno.

ISIG - IBM Security Identity Governance

Compliance, Audit e Controllo rischio accessi

Apporta i seguenti benefici:

- la Riduzione dei rischi.
- Rispetto delle politiche di sicurezza.
- Gestione della conformità alle normative.
- Riduzione dei costi di amministrazione IT e dei costi di preparazione degli audit.
- Definizione e applicazione di politiche unificate di accesso ai dati.
- Automatizzazione dei processi di remediation/compensazione del rischio.
- Memorizzazione a fini di audit di tutte le transazioni relative all'erogazioni e gestione di permessi di accesso.
- Promozione della consapevolezza e tracciabilità nella gestione delle autorizzazioni concesse agli utenti.

ISIG - IBM Security Identity Governance

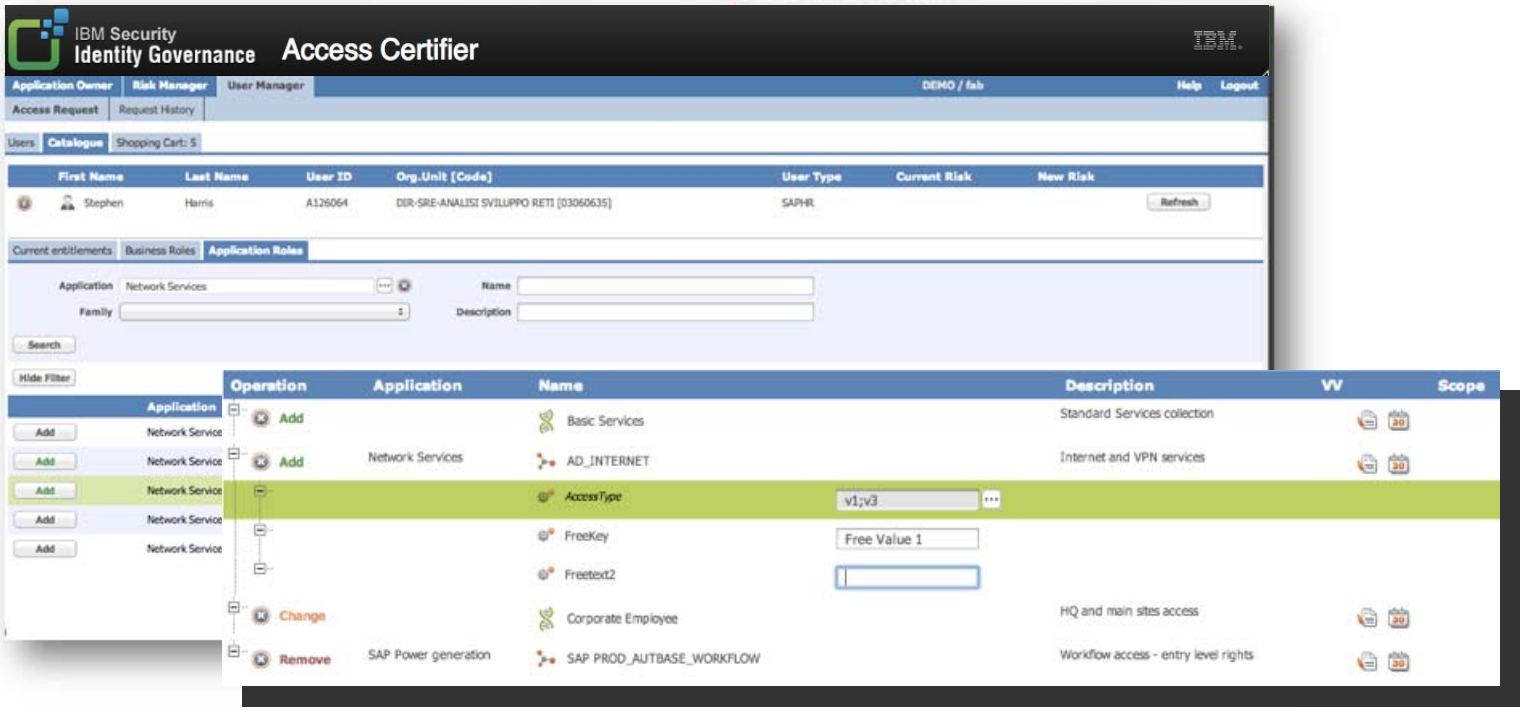
Funzionalità erogate

Visibilità	Verifica profili	Segregazione dei compiti	Gestione ruoli	Access Request
Chi ha accesso a cosa?	Debbono ancora avere accesso a…?	Come rilevo e prevengo “combinazioni tossiche”?	Come modello e mantengo profile abilitativi coerenti con il principio “need to know”?	Come garantisco un processo di formale autorizzazione?

ISIG - IBM Security Identity Governance

Caso d'uso tipico: **Access Request Management** (requisiti chiave)

- Catalogo di profili autorizzativi gestito.
- Interfaccia semplice, «tipo Amazon».
- Capacità di prevenire rischi / combinazioni tossiche



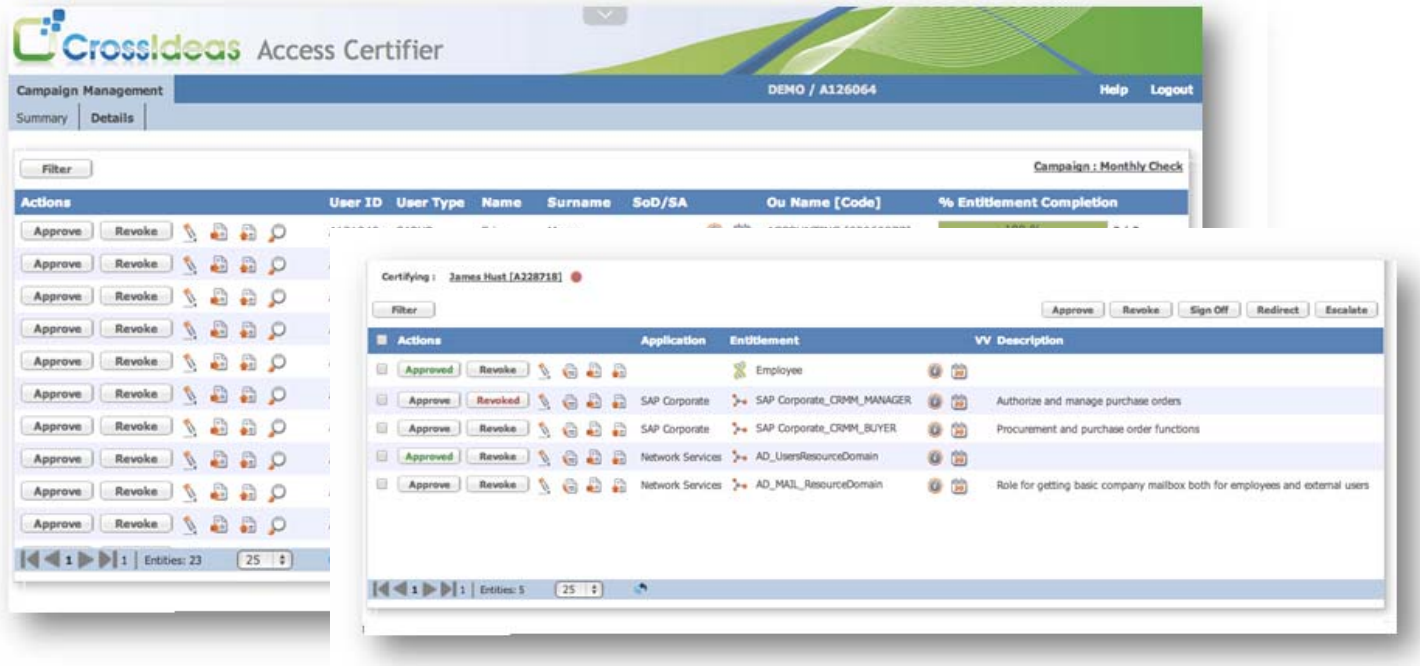
Premier Business Partner

ENGINEERING

ISIG - IBM Security Identity Governance

Caso d'uso tipico: **Access Certification** (requisiti chiave)

- Interfaccia semplice.
- Possibilità di creare campagne flessibili su base applicazione, unità org., filtri.
- Capacità di gestione processi di «sign-off» articolati.



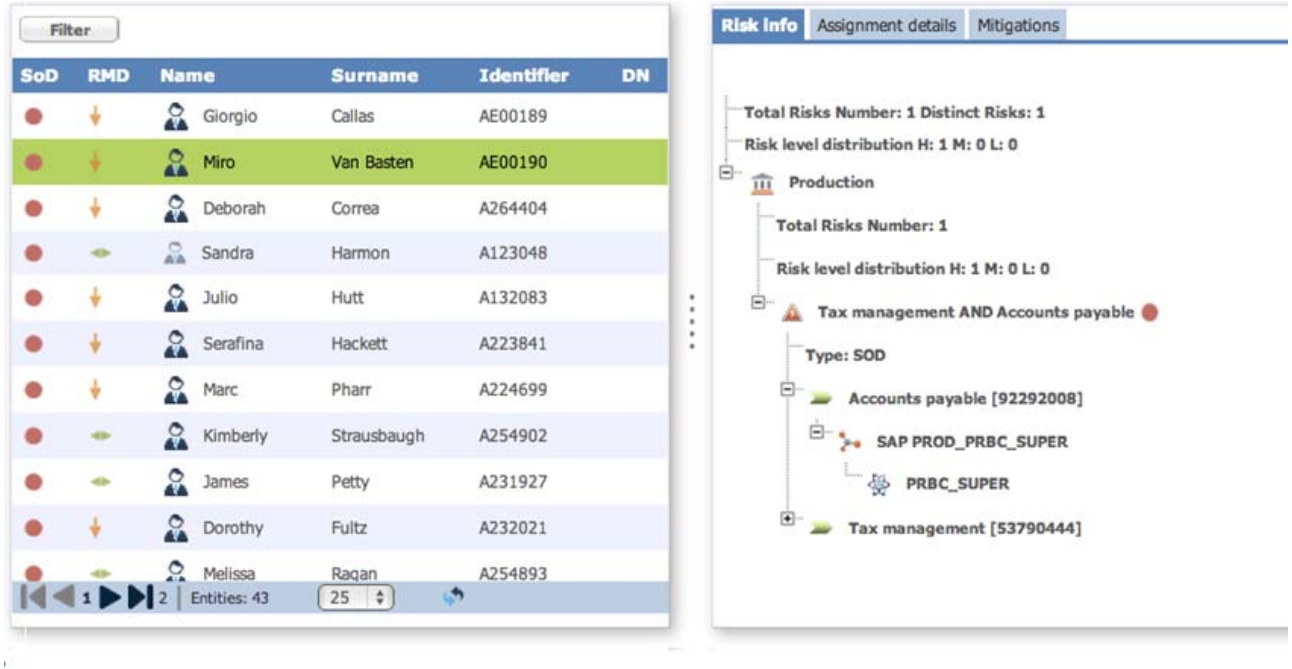
Premier Business Partner

ENGINEERING

ISIG - IBM Security Identity Governance

Caso d'uso tipico: **Segregation of Duty / Combinazioni tossiche** (requisiti chiave)

- «Motore» intelligente per modellare, rilevare e prevenire i rischi.
- Modellazione basata sulle attività di business, senza necessità di fare Ruoli.
- Capacità di catturare gli attributi applicativi.



ISIG - IBM Security Identity Governance

Gartner IGA Magic Quadrant 2014

IBM SECURITY IDENTITY GOVERNANCE

(IBM SECURITY SYSTEMS)

Premier Business Partner

ENGINEERING

ISIG - IBM Security Identity Governance

Case history / Informatica Trentina

Soluzione di Identity & Access Management per la Provincia Autonoma di Trento

Il progetto ha come obiettivo la gestione dell'identità digitale di tutti i dipendenti degli Enti e della pubblica amministrazione locale della Provincia di Trento che hanno la necessità di accedere alle risorse informatiche della Provincia.

La soluzione proposta comprende sia la soluzione ISIM, per la gestione dell'identity management e autentication, sia la soluzione ISIG (ex prodotto IDEAS di CrossIdeas) per la gestione dell'identity governance.

- 6.500 utenti interni (dipendenti enti e Pal Provincia di Trento)
- Circa 200 applicazioni gestite

ISIG - IBM Security Identity Governance

Case history / Ministero della Salute

MINISTERO DELLA SALUTE

Soluzione per la gestione del controllo accessi e delle identità digitali degli utenti del servizio NSIS – Nuovo Sistema Informativo Sanitario

La soluzione adottata (ISIG ex Ideas) permette la completa gestione dell'Identity and Access Management degli utenti NSIS.

Questi utenti sono i dipendenti e i consulenti del Ministero della Salute e tutti gli altri utenti che per la propria attività professionale hanno necessità di interagire con i servizi NSIS.

- 3.500 utenti interni (dipendenti e consulenti Ministero della Salute)
- c.a 20.000 utenti esterni (no cittadini)
- Circa 100 applicazioni gestite

Premier Business Partner IBM

ENGINEERING

ISIG - IBM Security Identity Governance

Case history / Ministero della Salute

Comune di Milano

Soluzione per la gestione del controllo accessi e delle identità digitali degli utenti del Comune di Milano.

La soluzione ISIG (ex Ideas) permette la gestione dell'identità digitale di tutti gli utenti che accedono ai servizi del portale.

Questi utenti possono essere tutti i cittadini che hanno necessità di usufruire di questi servizi.

- 20.000 utenti (cittadini registrati al servizio)

Premier Business Partner IBM

ENGINEERING

@EngineeringSpa