L'impatto della governance sui programmi di gestione delle identità

Rafael Etges, CISA, CRISC, CIPP/C, CISSP, è responsabile dei servizi di consulenza di IT Security presso TELUS, dove dirige le attività di governance, risk management e compliance (GRC) dell'organizzazione nonché i servizi di consulenza legati alla gestione delle identità e degli accessi. È membro dell'ISACA Toronto (Ontario, Canada) Chapter.

Anderson Ruysam, CRISC, CISSP, ITIL, è senior IT risk advisor presso il Governo dell'Ontario, Canada, specializzando in IT GRC e business management. Ruysam vanta oltre 14 anni di esperienza nelle attività di IT governance, risk management e security.

Recentemente, l'interesse dimostrato dalle organizzazioni nelle iniziative relative alla gestione delle identità e degli accessi è cresciuto notevolmente principalmente a causa delle preoccupazioni manifestate da parte dei governi e delle imprese nel settore retail e finanziario riguardo alla perdita di dati, alle frodi e alla conformità alle normative, nonché come conseguenza dell'interesse del management nell'ottimizzazione dei processi IT e nella riduzione dei costi. I benefici associati ai programmi di gestione dei ruoli e delle identità includono una migliore gestione degli accessi ai dati e ai sistemi informativi (IS), che comporta una più elevata sicurezza e miglior risk management; la trasferibilità e la possibilità di riutilizzare le definizioni dei ruoli in tutta l'organizzazione; la capacità di rispettare e dimostrare la conformità alle normative; una migliore business continuity e, altrettanto importante, l'ottimizzazione dei costi legati all'amministrazione e all'integrazione degli applicativi aziendali.

Considerando che il budget medio annuo necessario alle imprese per l'implementazione delle soluzioni di gestione delle identità (IDM - Identity Management) sta per diventare a un numero a sette cifre [1], il significativo coinvolgimento e impegno del management è fondamentale per assicurare una corretta allocazione delle risorse. Oltre alla giustificazione di business per un simile investimento, è necessario che una solida governance dell'IDM sia applicata per assicurare che i rilevanti portatori di interessi siano coinvolti nella definizione dei principi e degli obiettivi alla base della gestione dei ruoli aziendali all'interno dell'organizzazione. Il messaggio costante deve evidenziare come l'IDM sia un problema aziendale che riguarda la compliance, i rischi, la privacy e l'ottimizzazione dei costi, così come il fatto che il principale driver rimane la corretta gestione dei ruoli e dei processi aziendali supportati da tecnologie complesse e non il contrario.

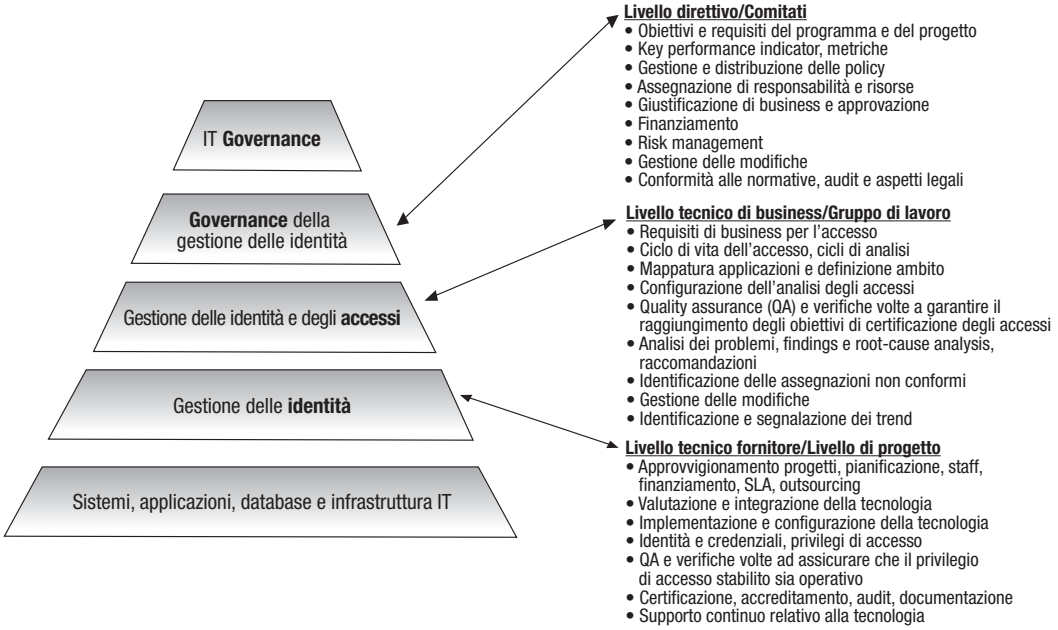
Questo articolo si focalizza su due domande: Quali sono gli elementi di governance necessari per garantire il successo di un'implementazione di un IDM all'interno di un contesto aziendale complesso? Qual è l'impatto finale dell'introduzione (o della mancata introduzione) di tali elementi?

GOVERNANCE DELL'IDM, DEI RUOLI E DEGLI ACCESSI

La disciplina della governance delle identità e degli accessi è in rapida evoluzione ed è in corso lo sviluppo di standard e best practice[2] Stanno avendo luogo numerosi dibattiti tra gli esperti di settore e talune best practice sono attualmente promosse da istituti di ricerca del calibro di Forrester[3], Burton Group[4] e Gartner,[5] che si concentrano inoltre su approcci, soluzioni e prodotti in grado di soddisfare questi nuovi requisiti nelle rispettive aree di interesse.

Sta nascendo una nuova e variegata terminologia, sempre più utilizzata mano a mano che le pratiche applicative si sviluppano attorno alla gestione di ruoli, accessi e identità. In generale, il termine "ruolo" indica un insieme di responsabilità necessarie per eseguire operazioni o transazioni aziendali, con "accessi" si indicano i privilegi e le risorse utilizzate da chi riveste un determinato ruolo, mentre "l'identità" designa un individuo che ricopre un dato ruolo in un determinato momento.[6] Una chiara distinzione tra questi termini è di fondamentale importanza, in quanto la gestione di ciascuno di questi elementi sta dando vita a tre discipline distinte. Sebbene le soluzioni di gestione delle identità si focalizzino sulla fornitura e sulla revoca automatizzate delle identità/accessi alle risorse IT, esse sono poco efficaci in termini di governance degli accessi (quali ruoli dovrebbe ricevere l'accesso a quali risorse e come) e delle identità (come l'organizzazione definisce i ruoli e le identità con il coinvolgimento dei principali responsabili aziendali dei processi di business e di supporto che fanno affidamento sul funzionamento di tali ruoli).

Figura 1: esempio di framework per la gestione di ruoli e identità/accessi



La **Figura 1** mostra un esempio di framework utilizzato per differenziare tali elementi e per identificare necessità e requisiti di ciascun livello.

BENEFICI DELLA GOVERNANCE

Diverse entità e individui tendono a sostenere differenti interpretazioni e definizioni di governance. Secondo una definizione completa e imparziale di "governance aziendale": "La governance è costituita dal framework, dai principi, dalla struttura, dai processi e dalle pratiche poste in essere per indirizzare e monitorare la compliance e le prestazioni coerentemente con lo scopo e gli obiettivi complessivi di un'azienda"[7].

Le organizzazioni che per prime hanno implementato soluzioni di IDM per stimolare l'automazione e potenziare le proprie capacità di fornitura e revoca degli accessi nell'ambito IT devono ora far fronte a nuovi requisiti. Si trovano a dover sfruttare la stessa tecnologia per dimostrare la loro conformità agli standard e migliorare la trasparenza a quesiti quali "chi ha accesso a cosa?", "perché?" e "con l'approvazione di chi?" a un livello molto più dettagliato di quanto le soluzioni di IDM esistenti furono inizialmente progettate per offrire. Per soddisfare simili esigenze è necessario un livello aggiuntivo di governance relativo all'IDM. Tali requisiti sono, inoltre, correlati alla governance e alla compliance IT e riguardano direttamente le esigenze delle funzioni aziendali servite dall'IT.

I benefici derivanti dal fatto di riconoscere la necessità di livelli aggiuntivi di gestione della governance e degli accessi al vertice della tecnologia IDM sono molteplici e possono essere riassunti come segue.

- Automazione dell'intero processo di assegnazione e analisi dei ruoli, in linea con le esigenze e i requisiti di business definiti dai vertici aziendali e dai manager.
- Visibilità di tutti i privilegi di accesso degli utenti all'interno dell'intera azienda. Le analisi sono di facile comprensione per gli utenti aziendali e possono essere configurate per includere processi specifici.
- Supervisione mediante cruscotti con cui sono centralizzate e riconciliate varie informazioni di dettaglio per una comprensione immediata dello stato dei processi di analisi e certificazione.
- Certificazione e correzione delle assegnazioni agli utenti; certificazioni archiviate e completo audit trail delle modifiche cronologiche in grado di fornire l'evidenza richiesta dagli auditor.
- Integrazione con l'infrastruttura di gestione degli accessi agli utenti per tenere traccia di tutte le modifiche relative alle assegnazioni; definizioni dei ruoli e degli accessi semplificate in ogni fase del ciclo di vita dell'utenza.
- Work-flow delle richieste di modifica innescato da un cambiamento o da una revoca delle assegnazioni ovvero work-flow ad evento causati da un cambiamento che necessiti di un'analisi incrementale dell'accesso da parte di un utente.

L'implementazione della tecnologia IDM non è in grado di garantire da sola questi benefici e, in alcuni casi, il potenziale fornitore potrebbe promuovere in maniera eccessiva le capacità di

Vi interessa questo articolo?

- Leggere *Identity Management Audit/Assurance Program*:

  http://www.isaca.org/bookstore

- Per partecipare al programma *Gestione Identità* e ottenere maggiori informazioni a riguardo:

  http://www.isaca.org/topic-identity-management

tale tecnologia all'azienda. Senza supervisione, la tecnologia non è in grado di risolvere i problemi di business. I livelli di gestione degli accessi e di governance sono fondamentali per sfruttare appieno il valore dell'investimento realizzato, ma non sempre questo si verifica.

L'IMPATTO DELLA GOVERNANCE DELL'IDM SUI PORTATORI DI INTERESSE

La **Figura 2** mostra l'impatto positivo degli elementi di governance applicati nell'implementazione dell'IDM a beneficio dei vari portatori di interesse all'interno di un'organizzazione tipica.

CONCLUSIONI

Le soluzioni di IDM offrono una opportunità di creazione di valore straordinaria alle organizzazioni. Come altre tecnologie complesse, quali Customer Relationship Management (CRM) ed Enterprise Resource Planning (ERP), queste soluzioni influenzano il funzionamento dei principali processi di business aziendali. Ad un livello più alto rispetto al CRM e all'ERP, l'IDM è potenzialmente in grado di influenzare tutti i processi aziendali, in quanto i ruoli, le identità e gli accessi ai sistemi informativi sono gestiti dalla stessa soluzione. Inoltre, più la tecnologia si diffonderà all'interno dell'organizzazione, maggiore sarà il potenziale dell'IDM — implementata più o meno correttamente — di offrire un impatto positivo o negativo ai portatori di interesse.

Figura 2: impatto della governance delle identità e degli accessi sulle funzioni organizzative

Partecipante	Elementi di governance	Impatto
Chief information officer (CIO)	• Complessità ridotta • Produttività maggiore • Scalabilità • Costi ridotti • Migliore reattività agli audit	• Service desk - Visibilità e controllo degli utenti e delle modifiche agli accessi, apertura e chiusura dell'accesso; incidenza ridotta dei casi di reset delle password. • Ciclo di vita del software (SDLC, Systems Development Life Cycle) / Software come servizio (SaaS, Software as a Service) - Metodologie standardizzate per l'identificazione, l'autenticazione, l'autorizzazione e l'accesso di clienti e partner interni ed esterni; riutilizzo del codice. • Supporto IT - Database locali interni ai singoli sistemi eliminati e sostituiti da un centrale repository di accesso. Meno cicli e risorse necessari per mantenere e autorizzare l'accesso alle applicazioni e ai sistemi. • Auditing e compliance - Processi di gestione delle identità e degli accessi formalizzati, ripetibili, documentati e pronti per l'audit; riduzione dei costi di risposta agli audit.
Chief information security officer (CISO)	• Rischi gestiti a un livello accettabile • Implementazione e monitoraggio dei controlli	• Valutazioni dei rischi e dei controlli - Facilitati da regole chiare sull'accesso ai dati sensibili, abilitano una tempestiva identificazione delle violazioni.
Internal Audit	• Audit più rapidi con risorse limitate • Finding accurati • Attestazione migliore	• Ore di audit - Riduzione degli sforzi per la verifica indipendente dei controlli. • Evidenze automatizzate e affidabili. • Risultati di audit confrontabili - Rilevamento dei trend dei gap dei controlli, della responsabilità di tali gap nonché della loro azione di rimedio.
Business Lines	• Costi ridotti • Produttività maggiore • Redditività e risultati massimizzati • Prevenzione di frodi e perdite	• Cicli ridotti per revisioni di sistema, risoluzione dei problemi e QA delle analisi degli accessi. • Congruenza nelle regole di accesso agli applicativi aziendali. • Possibilità di visualizzare chi può accedere ai dati aziendali in qualsiasi momento. • Riduzione di frodi e perdite causate dall'errata configurazione delle regole di accesso, ancorché la sola tecnologia IDM non è in grado di prevenire.
Chief financial officer (CFO)	• Massimizzazione dei ricavi • Gestione dei costi • Ottimizzazione redditività • Massimizzazione del valore creato agli azionisti • Migliore conformità ed efficienza nei processi di compliance, audit e assunzione responsabilità	• Spese operative ridotte - Organico ottimizzato, spese di consulenza/outsourcing ridotte. • Budgeting - Riduzione delle richieste di risorse *ad hoc*/di emergenza causati dalla scarsa visibilità dei sistemi e della infrastruttura IT. • Riduzione dei rischi - Attuazione della segregazione dei compiti e dei requisiti di due diligence. • Audit accelerati, costi di audit ridotti e finding accurati e prevedibili.

Il fattore che più di ogni altro influisce su questi risultati è la governance. I fornitori di tecnologie non sono in grado di comprendere appieno i problemi di business che determinano un'organizzazione ad acquisire una soluzione di IDM e non hanno una conoscenza approfondita dei processi di business aziendali o le competenze necessarie per integrare e adattare i suoi sistemi esistenti a tale soluzione. L'organizzazione deve essere preparata a valutare le proprie capacità e i propri gap rispetto alle best practice in materia di gestione di ruoli e delle identità all'interno di aree quali la certificazione degli accessi, la gestione delle assegnazioni, la richiesta degli accessi, il monitoraggio e le segnalazioni. Deve, inoltre, essere pronta a dare priorità alle misure volte a colmare questi gap.

A un livello molto elevato, le principali aree di attività includono la stesura di un documento programmatico (i.e. piani di comunicazione, responsabilità), la determinazione dei processi da considerare e l'identificazione dei ruoli e dei sistemi informativi associati, delle policy applicabili e dei relativi standard da attuare da parte degli esperti selezionati all'interno dell'organizzazione e coordinati da un program manager che si confronta con le aree aziendali interessate.

Anche la tempistica può rivelarsi un fattore critico: se la soluzione venisse implementata troppo presto, potrebbe non essere compresa dalla comunità degli utenti e dalla funzione IT; se invece venisse implementata troppo tardi, l'investimento potrebbe non dare frutti entro le scadenze previste. L'implementazione della tecnologia, l'adattamento dei processi, l'apprendimento e l'acquisizione di conoscenze, la supervisione e la gestione devono essere scrupolosamente sincronizzate per garantire la buona riuscita dell'implementazione dell'IDM.

Questi elementi non sono semplici da gestire; tuttavia, se vengono incluse nel processo di pianificazione e debitamente considerate durante tutte le fasi dell'implementazione, le soluzioni di gestione delle identità e degli accessi si riveleranno immensamente fruttuose per quelle organizzazioni che si affidano alla tecnologia per creare valore.

NOTE FINALI

[1] Kampman, Kevin; "Role Management in the Enterprise: Street Scenes", Burton Group, 23 agosto 2007, *www.burtongroup.com/Research/PublicDocument.aspx?cid=1126*

[2] Identity Management Forum, The Open Group, *www.opengroup.org/idm*

[3] Cser, Andras; Bill Nagel; Stephanie Balaouras; Nicholas M. Hayes; "Identity and Access Management Adoption in Europe: 2009—Uptake of Individual Technologies Is Low, But Cloud Options Hold Promise", Forrester Research, 14 maggio 2010, *www.forrester.com/rb/Research/identity_and_access_management_adoption_in_europe/q/id/56811/t/2*

[4] Kampman, Kevin; "Characteristics of an Effective Identity Management Governance Program", Burton Group, 22 gennaio 2010, *www.burtongroup.com/Research/PublicDocument.aspx?cid=1731*

[5] Consultare i discorsi di apertura e la sessione "IAM Foundations: Assessing the Maturity of Your IAM Program" del Gartner Identity & Access Management Summit del 2010, *www.gartner.com/technology/summits/na/identity-access/index.jsp.*

[6] Questi termini sono in corso di definizione da parte degli autori per quanto concerne il presente articolo. Nel settore è utilizzata un'etimologia differente, a conferma della mancanza di maturità e chiarezza in merito alle discipline di gestione di identità e accessi.

[7] Stachtchenko, Patrick; "Taking Governance Forward", *ISACA Journal*, vol. 6, 2008, *www.isaca.org/archives*