

Identity Governance & Administration

La soluzione

La soluzione **Identity Governance and Administration** permette di gestire in maniera centralizzata le identità e i relativi accessi alle applicazioni, controllandone la profilatura. Permette inoltre di gestire e monitorare i rischi legati agli accessi applicativi, come ad esempio **accessi sensibili** o **permessi** in violazione delle regole di “*Segregation of Duties*”. La soluzione offre un sistema di workflow approvativi da sfruttare in fase di richiesta di nuovi permessi, dando evidenza immediata di eventuali violazioni delle politiche aziendali, gestendo eventuali ulteriori passaggi approvativi in caso di necessità.

Attraverso l'**Identity Governance and Administration** è anche possibile avviare campagne di ricertificazione per garantire sempre il principio del “Least Privilege”, secondo cui un utente deve accedere ai sistemi con il minimo numero di permessi che gli permettano di lavorare correttamente.

La piattaforma consente infine la produzione di **Audit Report** costantemente aggiornati utilizzando i dati raccolti grazie alla applicazione.

A chi è rivolto?

La soluzione è rivolta ad aziende e Pubbliche Amministrazioni con necessità di automazione di flussi di provisioning (gestione e distribuzione delle risorse software) e la gestione del ciclo di vita degli utenti, ma anche a clienti con necessità di governance e compliance, non necessariamente legate all'automazione dei processi.

Si adatta sia a clienti che già hanno una piattaforma in esercizio che a clienti che si avvicinano all'implementazione di una nuova piattaforma di Identity Governance.



Come erogiamo il servizio

Cybertech offre 2 tipi di servizio:

1. Servizio di installazione, configurazione e messa in opera della piattaforma e successiva gestione in modalità SaaS (Software as a Service) o On Premise.
2. Servizio di gestione della piattaforma esistente del cliente, mettendo a disposizione le nostre competenze attraverso gli servizi erogati dalla **Control Room Cybertech** o il supporto dei nostri esperti On Premise (presso le strutture del cliente).



Perché Identity Governance and Administration

- Per automatizzare i processi di provisioning e di gestione del ciclo di vita degli utenti;
- Per mantenere sotto controllo il livello di rischio legato agli accessi applicativi;
- Per usufruire di report chiari e aggiornati sullo stato delle identità e degli account;
- Per sottoporre a revisione periodica, tramite campagne di certificazione gli account e i permessi assegnati agli utenti, tenendone traccia in un'unica console.





Punti di forza

1. I servizi di **Identity Governance & Administration** consentono in una console unica di:
 - gestire identità a livello centralizzato;
 - gestire processi di governance, le identità e gli accessi;
 - tenere costantemente sotto controllo lo stato di rischi correlato.
2. Possibilità di integrazione con software esterno.
3. Possibilità di integrazione out of the box della piattaforma con le soluzioni presenti sul mercato.



Vantaggi

- Soluzione chiavi in mano (SaaS);
- Gestione remota della piattaforma;
- Disponibilità del centro di competenze Cybertech.

Opzioni del servizio	Bronze	Silver	Gold
Metriche della fornitura (Ambiente di Produzione)			
Numero di utenti	Fino a 1000	Fino a 5000	Più di 5000
Number of APIs	Fino a 3	Fino a 5	Più di 5
Features (SaaS)			
Ambiente di Produzione	✓	✓	✓
Ruoli definiti	3	6	20
Provisioning Automatico base	✓	✓	✓
Provisioning Manuale	✓	✓	✓
Definizione profili accesso alla GUI (HD, End User, Manager)	✓	✓	✓
Report per quarter su SLA e attività effettuate	1	2	5
Restore in case of failure to latest valid backup (1 backup every 24 hours – maintaining 3 days backup)	✓	✓	✓
Ambiente di Test	opzionale	opzionale	opzionale
Corrective Maintenance (1 year starting from production delivery)			
Support on delivered features	✓	✓	✓
Platform Monitoring	✓	✓	✓
Tickets per year	25	60	120



IBM Security Identity Governance & Administration

Con **IBM Security Identity Governance & Administration** si può:



Contribuire all'individuazione di aree di rischio e all'ottimizzazione degli accessi, fornendo insight visivi di inestimabile valore su utenti e comportamenti a rischio.



Consentire ai responsabili di rischi/ conformità di individuare rapidamente le violazioni mediante controlli SoD (Separation of Duty - Separazione delle mansioni).



Automatizzare processi che richiedono un intenso impiego di manodopera, ad esempio le certificazioni di accesso, le richieste di accesso la gestione e il provisioning di password per ridurre drasticamente i costi operativi.



Gestire richieste self-service per eseguire rapidamente l'onboarding, l'offboarding o la gestione dei dipendenti.



Fornire insight su utenti a rischio, limitando i rischi connessi.



Contribuire al raggiungimento della conformità normativa.



Prendere le decisioni appropriate per quanto riguarda gli accessi.



Per saperne di più visita il sito
www.cybertech.eu

