

PROGETTO GUIDATO S4L1

PRESENTED BY:

Guglielmo Carratello
Maria Huapaya
Luca Iannone
Giuseppe Pignatello
Mattia Chiriatti



OPZIONE 1: ARCHITETTURA DI RETE CON MIDDLEWARE ON-PREMISES

Descrizione Architettura:

- ERP-HQ è on-premises e accessibile solo agli utenti interni della sede centrale.
- ERP-BR è in cloud e accessibile tramite un portale web.
- Il middleware è on-premises e si collega a ERP-HQ tramite una VPN.
- Gli utenti della filiale si collegano a ERP-BR tramite internet.

Gestione della Sicurezza:

- Uso di VPN per la connessione sicura tra middleware e ERP-HQ.

OPZIONE 1: ARCHITETTURA DI RETE CON MIDDLEWARE ON-PREMISES

Passaggi di Implementazione :

1. Installazione e Configurazione del Middleware:

- Configurare il middleware on-premises.
- Assicurarsi che il middleware possa tradurre i dati tra ERP-HQ e ERP-BR.

2. Connessione VPN:

- Configurare una VPN per permettere al middleware di comunicare con ERP-HQ.

3. Accesso degli Utenti:

- Configurare l'accesso degli utenti interni alla sede centrale a ERP-HQ.
- Configurare l'accesso degli utenti della filiale a ERP-BR tramite un portale web.

OPZIONE 1: ARCHITETTURA DI RETE CON MIDDLEWARE ON-PREMISES

Vantaggi

- Sicurezza: Maggiore controllo sulla sicurezza dei dati poiché il middleware è on-premises.
- Riservatezza: Minore esposizione dei dati sensibili su internet.

Svantaggi

- Manutenzione: Maggiore complessità nella gestione e manutenzione dell'infrastruttura on-premises.
- Scalabilità: Potrebbe essere più difficile scalare rispetto a una soluzione completamente cloud.

OPZIONE 2: SOSTITUZIONE DEL MIDDLEWARE CON UNA SOLUZIONE SAAS/IPAAS

Architettura:

- Sostituzione del middleware con una soluzione SaaS/iPaaS per l'integrazione dei dati.
- Possibile utilizzo di soluzioni low-code/no-code per la gestione dei dati e la sincronizzazione tra ERP-HQ e ERP-BR.
- Le soluzioni SaaS/iPaaS proposte includono Azure Data Factory, ByteRoute, Airbyte, Dataddo, Marjory.

OPZIONE 2: SOSTITUZIONE DEL MIDDLEWARE CON UNA SOLUZIONE SAAS/IPAAS

Passaggi di Implementazione

- Selezione della Soluzione SaaS/iPaaS: Valutare e selezionare una soluzione SaaS/iPaaS adatta alle esigenze aziendali.
- Migrazione dei Dati: Migrare i processi di integrazione dei dati esistenti dal middleware attuale alla nuova piattaforma SaaS/iPaaS.
- Configurazione della Nuova Piattaforma: Configurare la piattaforma SaaS/iPaaS per gestire la sincronizzazione tra ERP-HQ e ERP-BR; Assicurarsi che la piattaforma gestisca correttamente la trasformazione e il mapping dei dati.

OPZIONE 2: SOSTITUZIONE DEL MIDDLEWARE CON UNA SOLUZIONE SAAS/IPAAS

Vantaggi

- Scalabilità: Maggiore facilità di scalabilità grazie alla natura cloud della soluzione SaaS/iPaaS.
- Manutenzione: Riduzione della complessità di gestione e manutenzione, poiché la responsabilità ricade sul fornitore del servizio.

Svantaggi

- Sicurezza: Potenziali preoccupazioni sulla sicurezza e privacy dei dati, in quanto i dati sono gestiti da un fornitore esterno.
- Dipendenza da Terzi: Dipendenza da un fornitore esterno per la gestione dell'integrazione dei dati.

THE BEST OPTION

Abbiamo scelto di adottare l'opzione 2, che prevede la sostituzione del middleware con una soluzione SaaS/iPaaS di data integration/automation, per diversi motivi chiave:

- Scalabilità: Le soluzioni SaaS/iPaaS offrono una scalabilità superiore rispetto alle soluzioni on-premises. Questo ci permette di adattare facilmente l'infrastruttura alle crescenti esigenze aziendali senza dover investire in costosi hardware e risorse IT.
- Riduzione dei Costi di Manutenzione: La manutenzione e l'aggiornamento dell'infrastruttura on-premises richiedono risorse significative in termini di tempo e denaro. Con una soluzione SaaS/iPaaS, il fornitore si occupa di queste attività, permettendoci di concentrare le risorse interne su altre priorità strategiche.
- Implementazione Rapida: Le piattaforme iPaaS offrono strumenti di integrazione low-code/no-code che consentono una configurazione e un'implementazione più rapide rispetto alle soluzioni tradizionali. Questo accelera il tempo di messa in opera e riduce il tempo necessario per iniziare a vedere i benefici dell'integrazione.
- Affidabilità e Uptime: I fornitori di soluzioni SaaS/iPaaS garantiscono alti livelli di uptime e disponibilità attraverso contratti SLA (Service Level Agreement), assicurando che i nostri sistemi siano sempre operativi e riducendo al minimo i tempi di inattività.
- Supporto e Assistenza: I fornitori di iPaaS offrono supporto tecnico e assistenza continua, riducendo il carico sul nostro team IT e garantendo una risoluzione rapida dei problemi.

ARCHITETTURA iPaaS:

1.

Azure Data Factory (ADF):

- Creeremo un'istanza di Azure Data Factory nel tenant Azure dell'azienda, utilizzando le risorse di calcolo e archiviazione appropriate.

2.

Connettività:

- Configureremo connettori sicuri per accedere agli ERP HQ e BR, utilizzando autenticazione basata su credenziali crittografate.
- Utilizzeremo Azure Virtual Network per stabilire una connessione sicura tra Azure Data Factory e l'ERP HQ on-premises.

3.

Trasformazione dei dati:

- Implementeremo trasformazioni dei dati utilizzando l'attività Data Flow di Azure Data Factory, garantendo che i dati siano adeguatamente trasformati e armonizzati tra i due ERP.

4.

Automazione e monitoraggio:

- Pianificheremo e orchestreremo i flussi di lavoro di integrazione dei dati utilizzando trigger basati su orari o eventi.
- Utilizzeremo Azure Monitor per monitorare le attività di integrazione dei dati e rilevare eventuali anomalie.

5.

Sicurezza:

- Implementeremo il controllo degli accessi basato sui ruoli (RBAC) per garantire che solo gli utenti autorizzati possano accedere e modificare le risorse di Azure Data Factory.
- Utilizzeremo Azure Key Vault per gestire e proteggere le credenziali sensibili utilizzate nei connettori e nelle attività di integrazione dei dati.
- Abiliteremo il logging dettagliato e l'auditing per tenere traccia delle attività degli utenti e dei cambiamenti nelle risorse di Azure Data Factory.

6.

Backup e ripristino:

- Configureremo backup regolari dei dati del database su entrambi i lati (ERP HQ e BR).
- Utilizzeremo Azure Backup per eseguire backup regolari del database sul cloud, garantendo la protezione dei dati in caso di perdita o corruzione.
- Implementeremo una strategia di backup e ripristino su un database fisico per l'ERP HQ on-premises, utilizzando soluzioni di backup locali e la replica dei dati su un secondo sito sicuro.

Asset Name	IP Address	Asset Valuation	Site/Location	Team
Asset Name	IP Address	Asset Valuation	Site/Location	Team
Database		\$0 to \$100,000	On-Premises	Data Center & Storage, Database
ERP-BR		\$100,001 to \$200,000	Cloud	Branch Management, IT Systems Management
ERP-HQ		\$400,001 to \$500,000	On-Premises	IT Systems Management
ETL		\$0 to \$100,000	On-Premises	IT Systems Management
Information		\$400,001 to \$500,000	Cloud, On-Premises	Information Security
Personnel		\$200,001 to \$300,000	On-Premises	
Website		\$400,001 to \$500,000	Cloud	Information Security, IT Systems Management, Network, Web Systems

Una volta stabiliti gli asset fondamentali per l'azienda, possiamo procedere al risk assessment.

The screenshot shows the SimpleRisk platform interface. At the top, there are two tabs: 'Frameworks' (which is active) and 'Controls'. Below the tabs, there is a summary bar with a plus icon and the text 'Active Frameworks (2)' and 'Inactive Frameworks (0)'. A table follows, with columns 'Framework Name' and 'Framework Description'. Two rows are listed: 'NIST SP800-30r' and 'NIST SP 800-53'. On the left side of the screen, there is a vertical sidebar with three numbered steps: 1. Define Control Frameworks (highlighted in red), 2. Document Program, and 3. Define Exceptions.

Framework Name	Framework Description
NIST SP800-30r	
NIST SP 800-53	

Come da richieste, abbiamo caricato
in piattaforma SimpleRisk la
documentazione per i framework di
riferimento: NIST SP 800-30r e NIST SP
800-53

The diagram illustrates the third step of a three-step process: Document Program. On the left, a vertical sidebar shows three steps: 1 Define Control Frameworks, 2 Document Program (highlighted in red), and 3 Define Exceptions. The main area features a table for managing documents, with columns for Document Name, Document Type, Control Frameworks, Controls, Creation Date, Approval Date, and Status. The table contains four rows of data.

Document Name	Document Type	Control Frameworks	Controls	Creation Date	Approval Date	Status
Architecture	guidelines			05/20/2024		Draft
NIST SP 800-53r	guidelines			05/20/2024		Draft
NIST SP 800-30r	standards			05/20/2024		Draft
NIST SP 800-53	standards			05/20/2024		Draft

Successivamente, abbiamo provveduto a caricare i documenti come guidelines o standards.

The screenshot shows a configuration interface with the following fields:

- Next Review Date Uses: Inherent Risk
- HighCharts Delivery Method: HighCharts CDN
- jQuery Delivery method: jQuery CDN
- Bootstrap Delivery Method: jsDelivr CDN
- SimpleRisk Base URL: https://192.168.1.92
- Risk Appetite: Low (2) (indicated by a yellow square)

A horizontal slider bar is present below the risk appetite field, with a white square handle positioned between the yellow and orange segments. A large black rectangular redaction box covers the top portion of the interface.

Update

Impostato il livello di risk appetite a 2, possiamo procedere con la mitigazione del rischio. Il valore di partenza del rischio legato ad accessi non autorizzati è pari a 6.4 inizialmente.

The screenshot shows a risk management application interface. At the top left, there are two colored boxes: an orange 'Inherent Risk' box containing '6.4' and 'Medium', and a yellow 'Residual Risk' box containing '1.92' and 'Low'. To the right, the 'ID #' is listed as '1001' and the 'Status' is 'Mitigation Planned'. Below this, the 'Subject' is 'Accesso non autorizzato' with an edit icon. Underneath, there are two links: 'View Risk Scoring Details' and 'Show Risk Score Over Time'. A navigation bar at the bottom includes 'Details' (in red), 'Mitigation' (selected), and 'Review'.

The main area contains several input fields and dropdown menus:

- Mitigation Submission Date: 05/20/2024
- Planned Mitigation Date: 06/01/2024
- Planning Strategy: Mitigate
- Mitigation Effort:
- Mitigation Cost:
- Mitigation Owner:
- Mitigation Team:
- Mitigation Percent:
- Mitigation Controls: A dropdown menu titled 'Select for Mitigation Controls' lists seven items with checkboxes:
 - AC-3: Access Enforcement
 - AC-6: Least Privilege
 - AC-7: Unsuccessful Login Attempts
 - AU-6: Audit Review, Analysis, and Reporting
 - IA-2: Identification and Authentication
 - IA-3: Device Identification and Authentication
 - IA-4: Identifier ManagementThe status 'All selected (7)' is shown at the bottom of the dropdown.

On the right side, there are two sections: 'Current Solution:' and 'Security Requirements:', each containing a text input field with rich text editing tools (bold, italic, underline, etc.) and a placeholder text 'MFA, IAM'.

A large black rectangular redaction box covers the bottom half of the page content.

Nella figura affianco, i controlli implementati

Inherent Risk: 6.4 (Medium) | Residual Risk: 3.2 (Low)

ID #: 1001 | Status: Mitigation Planned | Subject: Accesso non autorizzato

Risk Mapping: Privilege escalation, Unauthorized access, Data loss / corruption, System compromise, Information loss / corruption due to technical attack, Lack of a security-minded workforce

Threat Mapping: Hacking & Other Cybersecurity Crimes

Submission Date: 05/20/2024 | Submitted By: babbo

Category: Access Management | Risk Source: External

Site/Location: All Sites | Risk Scoring Method: Classic

External Reference ID: | Current Likelihood: Likely

Control Regulation: NIST SP 800-53 | Current Impact: Major

Control Number: | Risk Assessment:

Affected Assets: Database, ERP-BR, ERP-HQ | Additional Notes:

Technology: Remote Access | Supporting Documentation: None

Team: Information Security, IT Systems Management

Additional Stakeholders: [Redacted]

Inherent Risk: 6.4 (Medium) | Residual Risk: 1.92 (Low)

ID #: 1001 | Status: Mitigation Planned | Subject: Accesso non autorizzato

Risk Mapping: Privilege escalation, Unauthorized access, Data loss / corruption, System compromise, Information loss / corruption due to technical attack, Lack of a security-minded workforce

Threat Mapping: Hacking & Other Cybersecurity Crimes

Mitigation Submission Date: 05/20/2024 | Current Solution: MFA, IAM

Planned Mitigation Date: 06/01/2024 | Security Requirements:

Planning Strategy: Mitigate | Security Recommendations:

Mitigation Effort: Considerable | Supporting Documentation: None

Mitigation Cost: \$0 to \$100,000

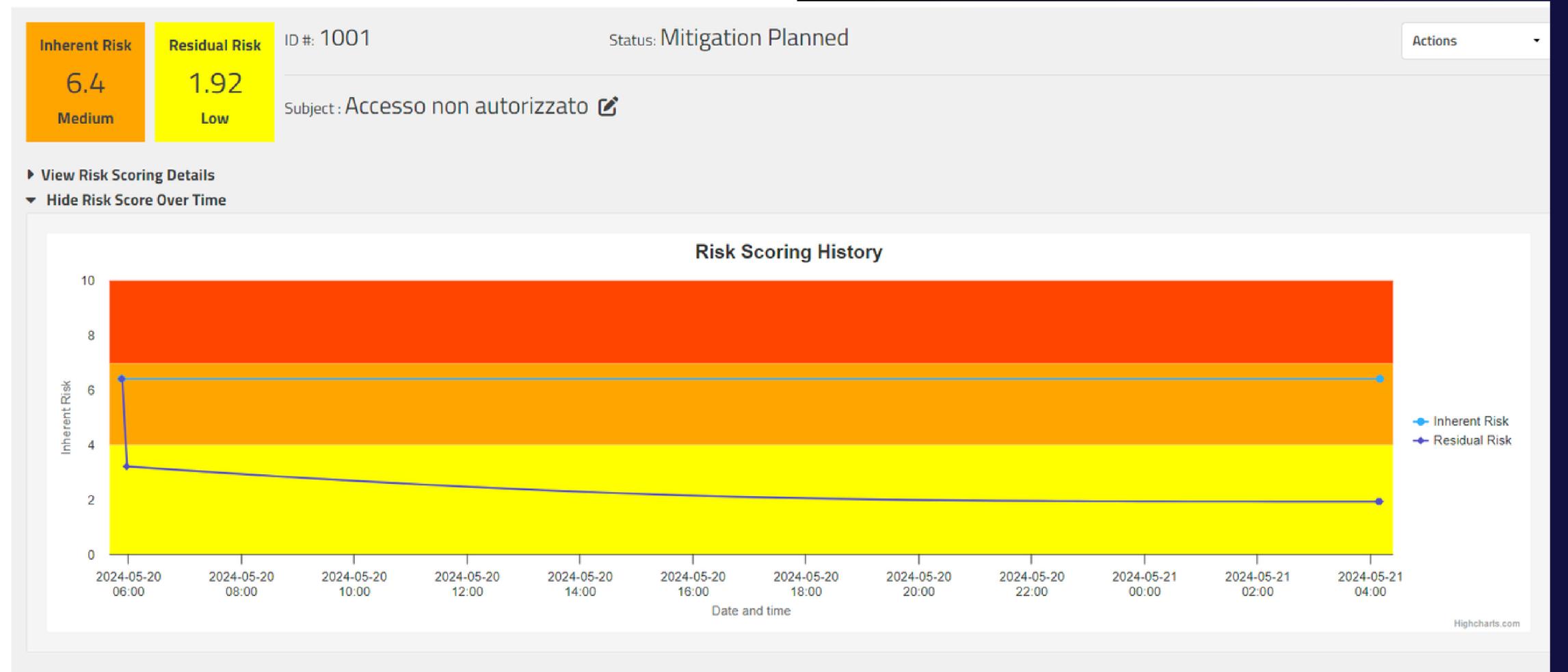
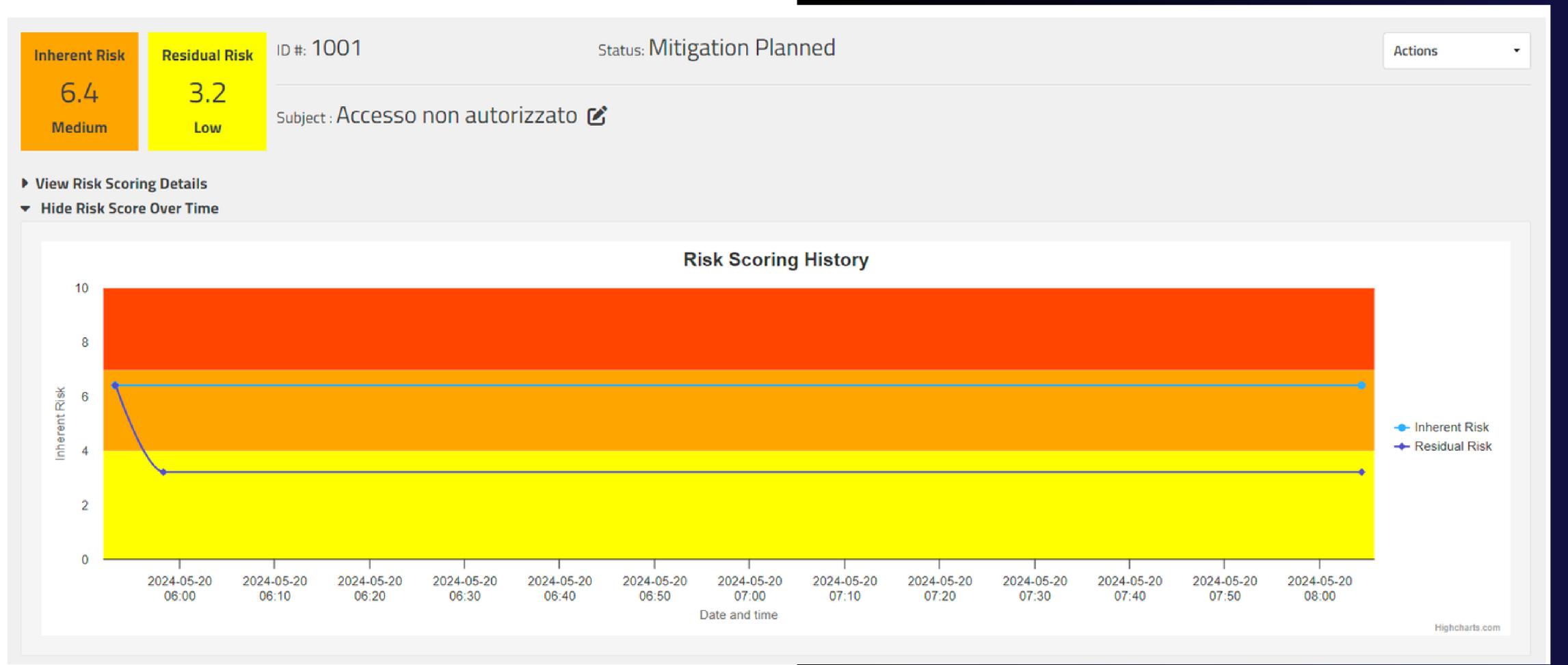
Mitigation Owner: babbo

Mitigation Team: Information Security, IT Systems Management

Mitigation Percent: 70% | Accept Mitigation

Implementati i controlli, possiamo procedere alla mitigazione del rischio.

I controlli effettuati, quindi, con le susseguenti soluzioni di implementazione di MFA e IAM, portano la percentuale di rischio a 1.92, quindi un livello accettabile.



Affianco, anche un grafico progressivo dei controlli implementati e di come il rischio vada mitigandosi fino a un livello accettabile (pari o inferiore a 2).

Valutazione del risk assessment

Prima dell'Implementazione dei Controlli Sicurezza dei Dati

Rischio Identificato: Elevato

Descrizione: L'infrastruttura on-premises per ERP-HQ, unita alla connessione tramite VPN, espone i dati sensibili a potenziali minacce interne ed esterne. La mancanza di controlli avanzati di accesso aumenta il rischio di accessi non autorizzati e possibili violazioni dei dati.

Manutenzione

Rischio Identificato: Elevato

Descrizione: La gestione e manutenzione dell'infrastruttura on-premises richiedono risorse significative, competenze tecniche elevate e costante monitoraggio. Questo aumenta il rischio di downtime, errori di configurazione e ritardi nella risoluzione dei problemi.

Scalabilità

Rischio Identificato: Medio-Alto

Descrizione: L'architettura on-premises presenta limitazioni strutturali e operative che rendono complessa la scalabilità per soddisfare le crescenti esigenze aziendali. Questo può portare a inefficienze operative e incapacità di respondere tempestivamente a nuovi requisiti di business.

Valutazione del risk assessment

Dopo l'Implementazione dei Controlli (MFA e IAM)
Sicurezza dei Dati

Rischio Ridotto: 1.92 (Accettabile)

Descrizione: L'implementazione di MFA (Multi-Factor Authentication) e IAM (Identity and Access Management) migliora significativamente la sicurezza dei dati, garantendo che solo utenti autorizzati possano accedere ai sistemi ERP. Questi controlli riducono drasticamente il rischio di accessi non autorizzati e aumentano la protezione contro le minacce esterne.

Manutenzione

Rischio Ridotto: Accettabile

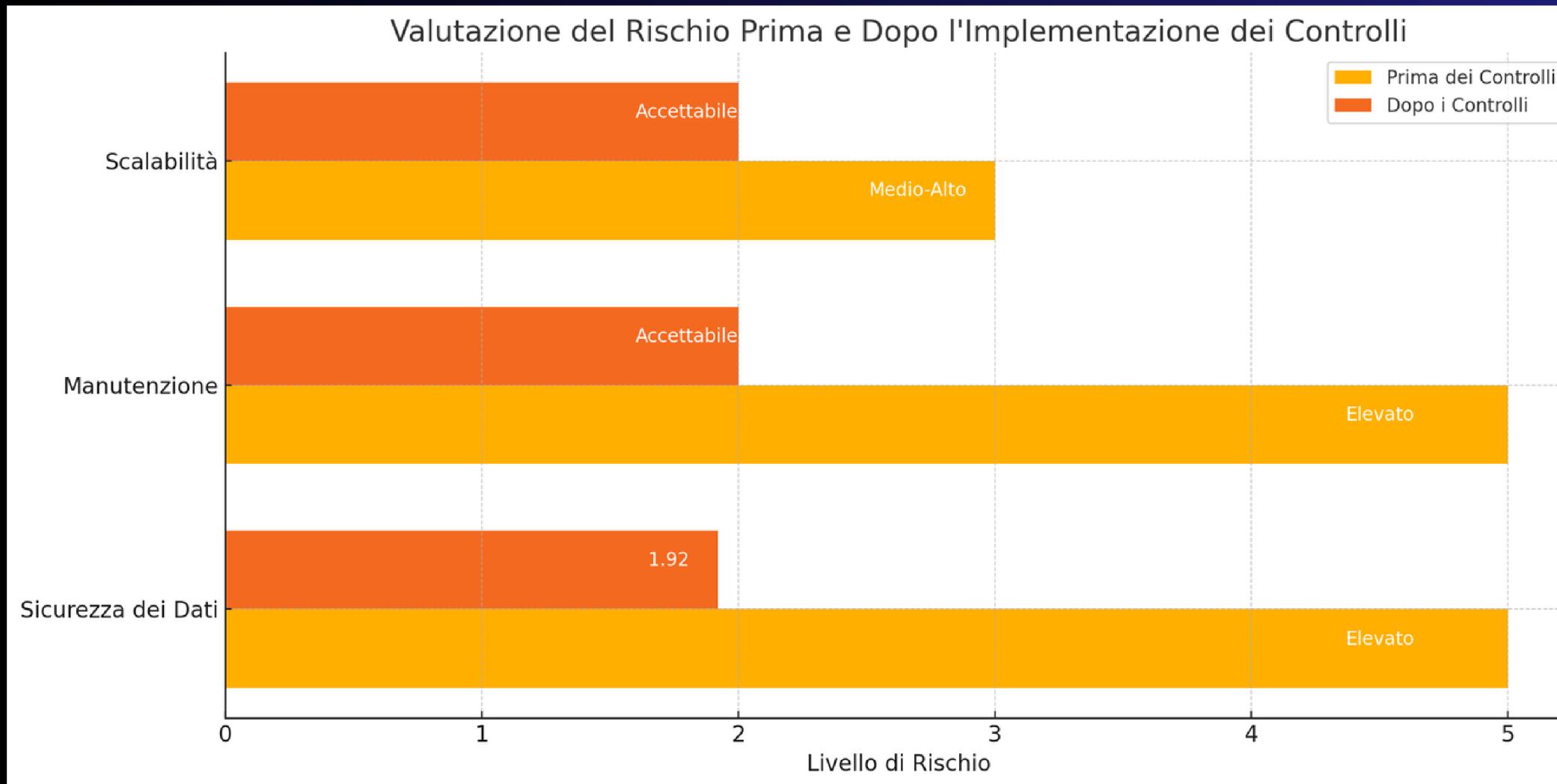
Descrizione: La migrazione verso soluzioni SaaS/iPaaS per l'integrazione dei dati trasferisce la responsabilità della manutenzione al fornitore del servizio. Questo riduce la complessità operativa e permette al personale IT di concentrarsi su attività strategiche piuttosto che su compiti di manutenzione ordinaria.

Scalabilità

Rischio Ridotto: Accettabile

Descrizione: Le soluzioni SaaS/iPaaS offrono una scalabilità intrinseca grazie alla loro natura cloud-based. Questo consente all'azienda di adattarsi rapidamente ai cambiamenti delle esigenze di business senza le limitazioni strutturali dell'architettura on-premises, migliorando l'efficienza operativa e la capacità di risposta.

Valutazione del risk assessment



Il grafico mostra in maniera riassuntiva il progresso dei controlli dopo l'implementazione di MFA e IAM.

Il grafico, quindi, confronta i livelli di rischio per le tre categorie evidenziate.

Valutazione del risk assessment

In Sintesi...

L'implementazione di controlli di sicurezza avanzati e la migrazione a soluzioni SaaS/iPaaS hanno ridotto significativamente i rischi legati alla sicurezza dei dati, manutenzione e scalabilità. Con un rischio residuo ridotto a 1.92 per la sicurezza dei dati e livelli accettabili per manutenzione e scalabilità, l'azienda può operare con maggiore fiducia e resilienza contro le minacce e le inefficienze.