

# Progetto S4/L1

## Gestione del rischio informatico per un caso aziendale specifico

**Alex Fiorillo**

**Andrea Dura**

**Angelo Di Mauro**

**Marco D'antoni**

**Marco Fasani**

**Sara Spaccialbelli**



# Introduzione

In questo progetto svilupperemo un piano di gestione del rischio informatico per un caso aziendale specifico che durerà tutta la settimana.

Faremo uso di **SimpleRisk** e seguiremo **NIST SP 800-37r2 RMF**, attraversando tutte le fasi:

- ▶ Prepare
- ▶ Categorize
- ▶ Select
- ▶ Implement
- ▶ Assess
- ▶ Authorize
- ▶ Monitor

Sono stati selezionati un sottoinsieme di task per far rientrare l'intero processo in una settimana.



# CASO AZIENDALE

Un'organizzazione ha sviluppato, in outsourcing, un'integrazione (middleware), tra il suo Enterprise Resource Planning (ERP) per la sede centrale (headquarter, HQ) e l'ERP di filiale (branch, BR), implementando un two-tier ERP.

### ERP

Software di gestione che integra tutti i processi aziendali e tutte le funzioni aziendali rilevanti, ad esempio vendite, acquisti, gestione magazzino, finanza o contabilità.

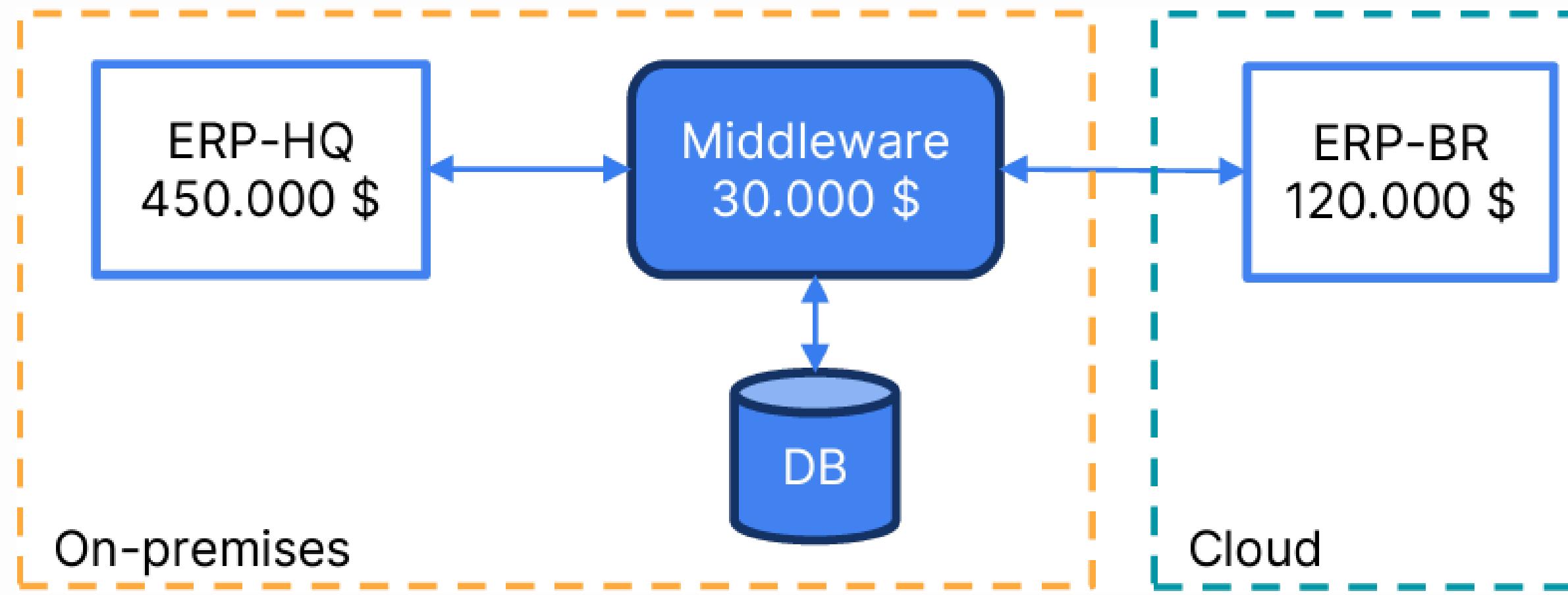
### TWO-Tier ERP

Approccio alla gestione delle risorse aziendali (ERP) che utilizza due sistemi software distinti per soddisfare le esigenze delle grandi aziende con molteplici sedi e/o filiali. Tier 1: ERP di sede centrale, centralizzato e robusto, in grado di gestire le operazioni e i requisiti generali dell'organizzazione. Tier 2: Nelle filiali o stabilimenti remoti viene implementato un sistema ERP separato. Questo sistema è più snello e flessibile, e permette alle filiali di avere una certa autonomia nella gestione delle loro operazioni, tenendo conto dei processi localizzati. Solitamente un ERP Tier 2 non è in grado di vedere gli altri ERP Tier 2.

### Middleware

Software che funge da intermediario tra diverse applicazioni, nel caso specifico sincronizzazione utenti, ordini e magazzino.

L'integrazione si è resa necessaria perché sono ERP di fornitori diversi e non esiste un'integrazione nativa. L'organizzazione non valuta di sostituire gli ERP.



# Specifiche middleware

L'organizzazione conosce il funzionamento di alto livello del middleware. All'interno del middleware è presente il modulo **Convert** che si occupa di tradurre i record dell'ERP-HQ in record validi per l'ERP-BR e viceversa.

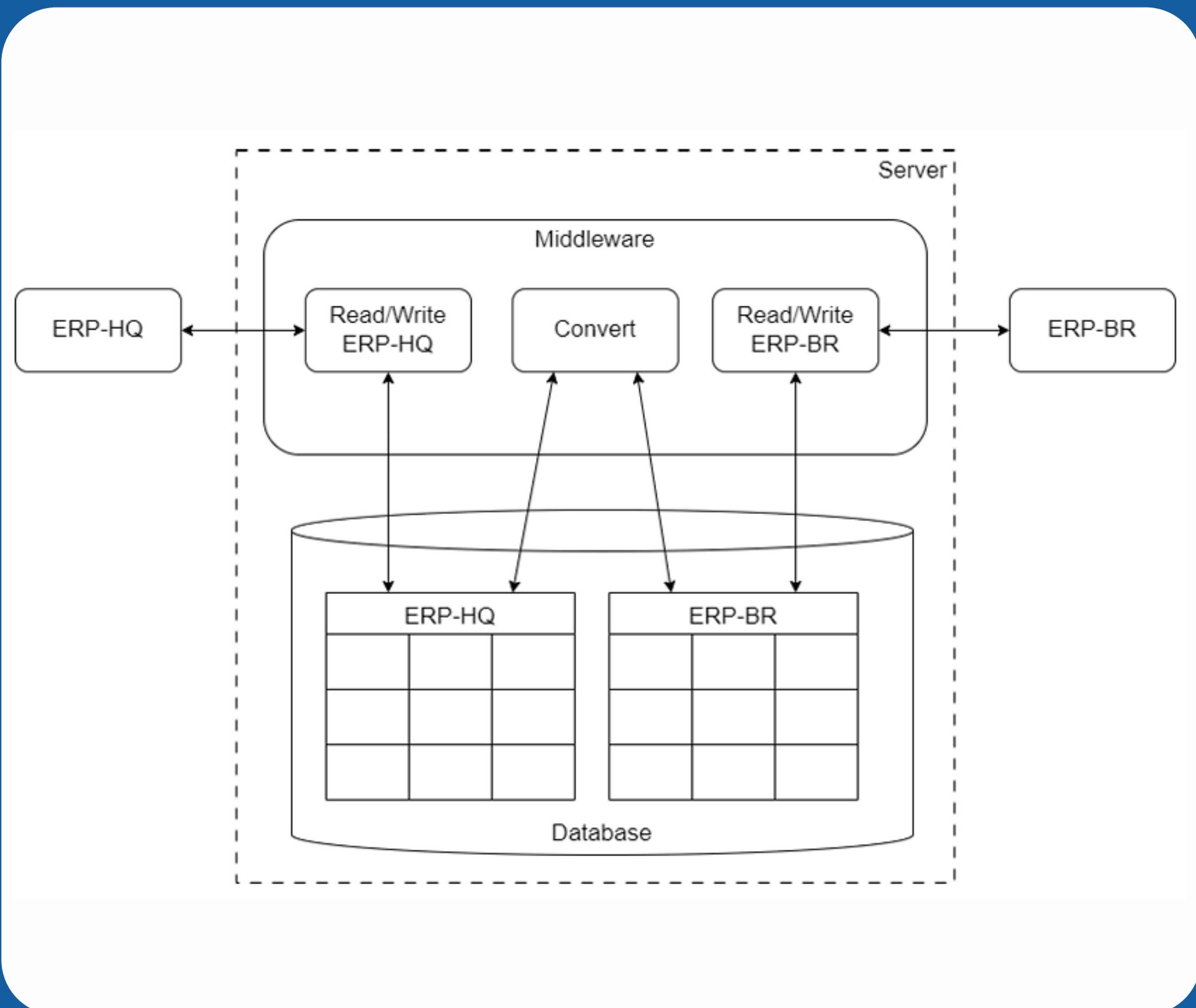
Convert si attiva quando rileva delle modifiche nelle tabelle del proprio database interno.

Nel database interno sono presenti le tabelle ERP-HQ e ERP-BR che conservano tutti i record che transitano tra ERP-HQ e ERP-BR (ERP-HQ e ERP-BR sono indipendenti e hanno un proprio database).

I due moduli Read/Write ERP-HQ e ERP-BR si occupano di leggere/scrivere i dati di transito nel db interno tra ERP-HQ/Middleware e ERP-BR/Middleware.

Middleware e database di supporto, risiedono sullo stesso server on-premises, ma differente dall'ERP-HQ.

Il Middleware riesce a soddisfare un carico massimo di 250 transazioni all'ora (tx/h) (complessive da/verso ERP-HQ/ERP-BR), l'attuale traffico si aggira sulle 100 tx/h.



# Scenario attuale

Da qualche giorno, l'azienda che sviluppato il middleware custom è stata chiusa, non offrendo più supporto e aggiornamenti. E' presente solamente il codice sorgente, non ci sono guide, manuali e progetti.

ERP-HQ e ERP-BR sono soluzioni proprietarie closed-source di altre aziende che continuano ad offrire supporto e aggiornamenti. ERP-HQ e ERP-BR non saranno oggetto di migrazioni (resteranno, rispettivamente, on-premises e su cloud).

Il middleware è di fondamentale importanza perchè permette di sincronizzare i due ERP, ad esempio, magazzino, impianti di produzione, utenti, fatturazione, ecc.

Adesso, l'**organizzazione deve valutare se:**

- ▶ **1.** continuare a manutenere questo middleware on-premises, di cui non conosce molto, trovando un nuovo fornitore in grado di fare un'analisi approfondita (compreso reverse engineering) per poterne continuare lo sviluppo, oppure,
- ▶ **2.** sostituire il middleware con una soluzione SaaS/iPaaS di data integration/automation, possibilmente low-code/no-code per evitare l'affidamento ad un'altra software house e gestire il solo mapping delle strutture dati con le risorse interne (dipendenti).

In occasione del riesame, si valuta anche la possibilità di aumentare le misure di sicurezza, se necessario.

Utilizzeremo **NIST SP 800-37r2 RMF** per impostare una strategia di gestione del rischio e dare un'indicazione al management/direzione su quale opzione, tra le due, è la più coerente rispetto al profilo organizzativo.

# Creazione dell'architettura di partenza (opzione 1)

Ipotizzate un'architettura di rete (fisica e logica) di partenza.

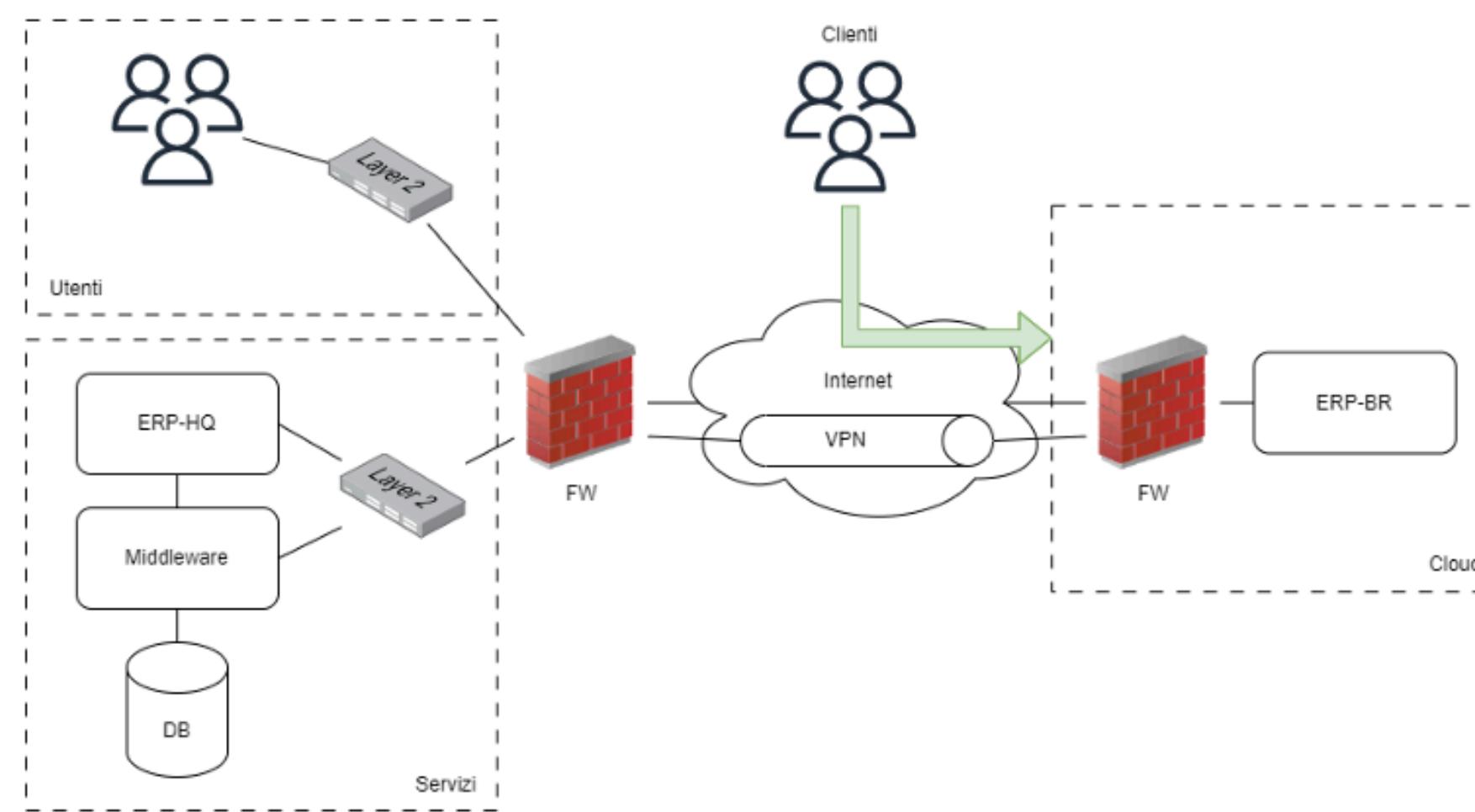
Ad esempio, nella figura mostrata in basso, i servizi sono in una rete separata rispetto agli utenti interni della sede centrale (HQ).

Gli utenti interni possono accedere all'ERP-HQ per la gestione interna e l'ERP-HQ può collegarsi a Internet solo per aggiornamenti (non per comunicare con l'ERP-BR).

Solo il middleware può collegarsi all'ERP-BR tramite VPN. I Clienti della filiale si collegano all'ERP-BR, in cui è presente un portale web.

Solo l'ERP-BR è in cloud.

Il CED on-premises non dispone di nessuna misura di continuità operativa (BC) se non un UPS per interruzioni elettriche di breve durata.



# Creazione dell'architettura alternativa (opzione 2)

Definite un'architettura che rispecchia gli obiettivi emanati dalla direzione nel **punto 2**:

Sostituire il middleware con una soluzione **SaaS/iPaaS** di data integration/automation, possibilmente low-code/no-code per evitare l'affidamento ad un'altra software house e gestire il solo mapping delle strutture dati con le risorse interne (dipendenti).

Scegliete una soluzione SaaS/iPaaS che permetta di riprodurre il funzionamento del Middleware, in particolare il modulo **Convert** che si occupa della trasformazione dei dati da una struttura dati ad un'altra (i rischi correlati all'utilizzo di un SaaS si equivalgono, basta sceglierne uno come riferimento).

Potete scegliere anche di indirizzarvi verso una soluzione opensource, in questo caso potrebbe essere a carico vostro la gestione dell'infrastruttura o della piattaforma cloud (IaaS/PaaS).

Esempi di data integration/pipeline/automation/ETL:

- <https://azure.microsoft.com/en-us/products/data-factory>
- <https://www.bytesroute.com/>
- <https://airbyte.com/>
- <https://dataddo.com/>



# Prepare - Organization Level

Dopo aver creato l'architettura di partenza e quella da valutare, avviate la fase Prepare di RMF. Concentratevi **solamente sui task in grassetto** (basta inserire una descrizione non troppo estesa). Dove richiesto, riportate i task su **SimpleRisk**. Per differenziare le entità relative a opzione 1 e 2, utilizzate i tag.

Task	Descrizione	SimpleRisk
TASK P-1 Risk Management Roles Identify and assign individuals to specific roles associated with security and privacy risk management.		
<b>TASK P-2 Risk Management Strategy Establish a risk management strategy for the organization that includes a determination of risk tolerance.</b>		Configurare i valori di rischio, matrici, formula, ecc.
TASK P-3 Risk Assessment—Organization Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis.		
TASK P-4 Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles (Optional) Establish, document, and publish organizationally-tailored control baselines and/or Cybersecurity Framework Profiles.		
TASK P-5 Common Control Identification Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems.		
TASK P-6 Impact-Level Prioritization (Optional) Prioritize organizational systems with the same impact level.		
TASK P-7 Continuous Monitoring Strategy—Organization Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.		

# ► Prepare - System Level

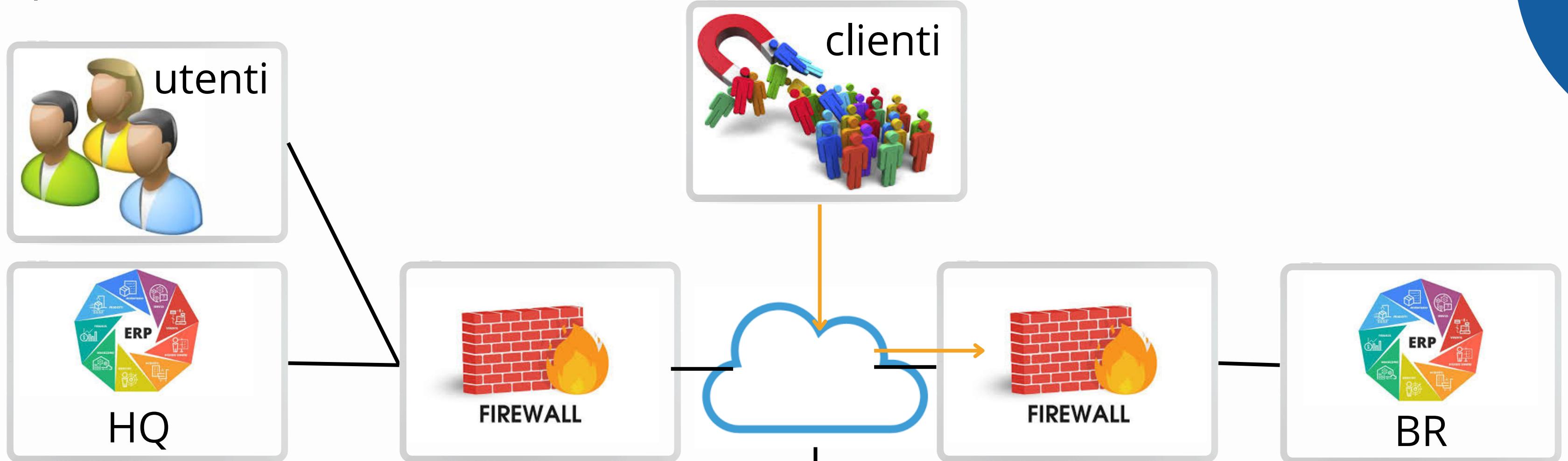
Task	Descrizione	SimpleRisk
<b>TASK P-8 Mission or Business Focus</b> Identify the missions, business functions, and mission/business processes that the system is intended to support.		
<b>TASK P-9 System Stakeholders</b> Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.		
<b>TASK P-10 Asset Identification</b> Identify assets that require protection.		Asset management*
<b>TASK P-11 Authorization Boundary</b> Determine the authorization boundary of the system.		
<b>TASK P-12 Information Types</b> Identify the types of information to be processed, stored, and transmitted by the system.		Anche le informazioni sono asset.
<b>TASK P-13 Information Life Cycle</b> Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system.		
<b>TASK P-14 Risk Assessment—System</b> Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.		
[...]		

\* Anche se i sistemi da gestire in SimpleRisk sono due (opzione 1 e 2), questi condividono molti componenti e i medesimi rischi (es. ERP-HQ e ERP-BR non variano). Inserite l'asset (o il rischio per l'esercizio di domani) una sola volta e utilizzate i tag per organizzarvi sull'applicazione (es. Opzione1, Opzione2, Entrambi).

# ► Prepare - System Level

Task	Descrizione	SimpleRisk
TASK P-15 Requirements Definition Define the security and privacy requirements for the system and the environment of operation.		
<b>TASK P-16 Enterprise Architecture Determine the placement of the system within the enterprise architecture.</b>		Creazione del sito, Asset management
TASK P-17 Requirements Allocation Allocate security and privacy requirements to the system and to the environment of operation.		
TASK P-18 System Registration Register the system with organizational program or management offices.		

# La proposta di rete



## Descrizione del Diagramma di Rete:

### ERP-HQ (On-premises):

API Gateway: Facilita la comunicazione sicura con il middleware SaaS/iPaaS.

Database Server: Archivia i dati aziendali cruciali.

VPN/SSL Gateway: Assicura che la connessione tra il server ERP-HQ e il middleware sia sicura.

### ERP-BR (Cloud):

API Gateway: Gestisce la sincronizzazione dei dati con il middleware SaaS/iPaaS.

Cloud Database: Memorizza i dati delle filiali.

Internet Gateway: Connessione sicura attraverso Internet.

### SaaS/iPaaS Middleware (Cloud):

Gestione API: Permette la comunicazione e sincronizzazione dei dati tra ERP-HQ e ERP-BR.

Data Mapping Tools: Facilita la configurazione e gestione dei dati tra i due ERP.

Gli utenti accedono ai rispettivi ERP tramite interfacce sicure, utilizzando le rispettive connessioni e autenticazioni IAM.

### Misure di Sicurezza:

Cifratura dei Dati: Tutti i dati in transito tra ERP-HQ, ERP-BR e il middleware SaaS/iPaaS devono essere cifrati.

Autenticazione Multi-Fattore (MFA): Implementare MFA per accedere ai sistemi ERP.

Monitoraggio Continuo: Utilizzare strumenti di monitoraggio per rilevare e rispondere a eventuali minacce o anomalie.

## Fase 1: Preparazione

### 1.1 Comprensione del contesto organizzativo e delle esigenze:

- Obiettivi aziendali: L'azienda vuole mantenere l'integrazione tra ERP-HQ e ERP-BR, assicurando continuità operativa.
- Vincoli: ERP-HQ e ERP-BR devono rimanere rispettivamente on-premises e su cloud. Non è possibile migrare o sostituire questi sistemi.
- Risorse: L'azienda dispone di risorse interne limitate e preferirebbe evitare di affidarsi completamente a terze parti.

## Fase 2: Categorizzazione del sistema

### 2.1 Identificazione del sistema:

- Sistema attuale: Middleware on-premises con capacità massima di 250 tx/h.
- Funzionalità critiche: Sincronizzazione dei dati tra ERP-HQ e ERP-BR, inclusi magazzino, produzione, utenti e fatturazione.

## Fase 3: Selezione dei controlli

### 3.1 Analisi delle opzioni:

- Opzione 1: Continuare a mantenere il middleware on-premises
  - Vantaggi: Maggiore controllo sul sistema, personalizzazione totale.
  - Svantaggi: Elevati costi e tempi per il reverse engineering, dipendenza da un nuovo fornitore per il supporto.
- Opzione 2: Sostituire il middleware con una soluzione SaaS/iPaaS
  - Vantaggi: Riduzione dei costi e dei tempi di manutenzione, facilità di gestione con soluzioni low-code/no-code, supporto continuo da parte del provider SaaS/iPaaS.
  - Svantaggi: Meno controllo diretto sul sistema, potenziali problemi di integrazione iniziale.

## Fase 4: Implementazione dei controlli

### 4.1 Implementazione per entrambe le opzioni:

- Opzione 1: Identificare un nuovo fornitore in grado di effettuare il reverse engineering e fornire supporto continuo.
- Opzione 2: Ricerca e selezione di una soluzione SaaS/iPaaS adatta, configurazione iniziale, formazione del personale interno per la gestione e manutenzione del sistema.

## Fase 5: Valutazione e autorizzazione

### 5.1 Valutazione dei rischi associati:

- Opzione 1: Rischio di alti costi e tempi per il reverse engineering e la manutenzione, dipendenza da un singolo fornitore per il supporto.
- Opzione 2: Rischio di perdita di controllo diretto e necessità di garantire la sicurezza e la conformità dei dati con il provider SaaS/iPaaS.

## Fase 6: Monitoraggio continuo

### 6.1 Monitoraggio e revisione continua:

- Opzione 1: Monitoraggio del rendimento del fornitore e aggiornamenti di sicurezza.
- Opzione 2: Monitoraggio delle performance del servizio SaaS/iPaaS, garanzia della conformità continua e valutazione delle SLA (Service Level Agreement).

## Raccomandazioni finali

### Analisi del profilo organizzativo:

- Costi e risorse: L'opzione 2 presenta un costo iniziale inferiore e richiede meno risorse interne per la gestione continua, essendo più adatta per un'organizzazione con risorse limitate.
- Sicurezza: La soluzione SaaS/iPaaS può offrire robusti meccanismi di sicurezza gestiti dal provider, riducendo l'onere sulla sicurezza interna.
- Flessibilità e scalabilità: SaaS/iPaaS offre maggiore flessibilità e scalabilità rispetto a una soluzione on-premises.

Conclusione: In base all'analisi effettuata utilizzando il framework NIST SP 800-37r2 RMF, raccomandiamo di sostituire il middleware con una soluzione SaaS/iPaaS. Questa opzione riduce i costi e i tempi di manutenzione, semplifica la gestione interna, e offre maggiore sicurezza e supporto continuo, allineandosi meglio con il profilo e le esigenze organizzative attuali.

Task	Descrizione
<b>TASK P-2 Risk Management</b> <b>Strategy Establish a risk management strategy for the organization that includes a determination of risk tolerance.</b>	<p>In questo contesto, la strategia deve garantire che l'adozione del servizio Azure rispetti le politiche di sicurezza e privacy dell'organizzazione e integri le considerazioni sulla gestione del rischio della catena di approvvigionamento (Supply Chain Risk Management, SCRM). Questo allineamento con il sistema di controllo della gestione del rischio aziendale garantisce che le decisioni strategiche dei dirigenti riguardo la gestione dei rischi di sicurezza e privacy, compresi quelli della catena di approvvigionamento, siano coerenti e ben informate.</p>
<b>TASK P-8 Mission or Business Focus</b> <b>Identify the missions, business functions, and mission/business processes that the system is intended to support.</b>	<p><b>Strategia di gestione del rischio:</b></p> <ul style="list-style-type: none"> <li><b>Identificazione dei rischi:</b> Valutare i rischi associati alle due opzioni (mantenere il middleware on-premises o passare a SaaS/iPaaS).</li> <li><b>Analisi dei rischi:</b> Analizzare la probabilità e l'impatto di ciascun rischio identificato.</li> <li><b>Mitigazione dei rischi:</b> Definire le misure per ridurre i rischi identificati.</li> <li><b>Monitoraggio continuo:</b> Implementare un sistema di monitoraggio per identificare e rispondere prontamente ai nuovi rischi.</li> </ul>

**Task****Descrizione**

**TASK P-9 System Stakeholders**  
**Identify stakeholders who have**  
**an interest in the design,**  
**development, implementation,**  
**assessment, operation,**  
**maintenance, or disposal of the**  
**system.**

- **Gli stakeholder in questo scenario includono:** Senior Executive (CEO/CIO): Responsabile dell'approvazione finale della strategia di gestione del rischio.
- Risk Manager: Coordina le attività di gestione del rischio, analizza i rischi e propone soluzioni.
- IT Manager: Implementa le soluzioni tecnologiche, monitora il sistema e garantisce la conformità con le politiche di sicurezza.
- Security Officer: Garantisce che le misure di sicurezza siano adeguate e monitorate costantemente.
- Compliance Officer: Assicura che tutte le soluzioni siano conformi alle normative vigenti.

**Task****Descrizione**

**TASK P-10 Asset Identification**  
Identify assets that require protection.

**Gli asset che richiedono protezione includono:**

- **Codice Sorgente del Middleware:** È essenziale proteggere il codice sorgente del middleware per garantire la continuità operativa e la sicurezza del sistema. Senza accesso al codice sorgente, la manutenzione e il miglioramento del sistema diventano difficili.
- **Dati nel Database Interno:** Il database interno contiene dati sensibili tra ERP-HQ e ERP-BR, e deve essere protetto per garantire riservatezza, integrità e disponibilità delle informazioni aziendali.
- **Funzionalità del Middleware:** Le funzionalità del middleware, specialmente il modulo Convert, sono critiche per la sincronizzazione dei dati tra i sistemi ERP. Devono essere protette per garantire la continuità operativa e la corretta trasformazione dei dati.
- **Architettura e Configurazione del Middleware:** L'architettura e la configurazione del middleware, comprese le impostazioni di sicurezza, devono essere protette da accessi non autorizzati per prevenire manipolazioni indebite che potrebbero compromettere la sicurezza e l'integrità del sistema.
- **Servizi di Data Integration/Automation SaaS/iPaaS:** Se si opta per una soluzione SaaS/iPaaS, i servizi di data integration/automation devono essere protetti per garantire la sicurezza e la corretta gestione dei dati durante il processo di integrazione.

**Task****Descrizione**

**TASK P-11**  
**Authorization Boundary Determine**  
**the authorization boundary of the system.**

**Il confine di autorizzazione del sistema in questo scenario comprende i componenti direttamente coinvolti nel processo di integrazione tra gli ERP HQ e BR, nonché l'infrastruttura di supporto necessaria per il funzionamento del middleware. In particolare, il confine di autorizzazione include:**

- Sistema di Middleware:** Questo include il software middleware stesso, compresi i suoi moduli per la trasformazione dei dati (come il modulo Convert), nonché eventuali componenti responsabili della lettura e scrittura nel database interno.
- Database Interno:** Il database utilizzato dal middleware per archiviare i record che transitano tra l'ERP-HQ e l'ERP-BR. Questo include le tabelle per i dati ERP-HQ e ERP-BR, nonché i moduli responsabili della gestione del flusso di dati tra gli ERP e il middleware.
- Infrastruttura del Server:** L'infrastruttura del server che ospita il middleware e il relativo database di supporto. Sebbene situata in locale, questa infrastruttura è separata dal sistema ERP-HQ, costituendo il proprio distintivo confine di autorizzazione.
- Interfacce di Integrazione:** Qualsiasi interfaccia o API utilizzata dal middleware per comunicare con i sistemi ERP, facilitando lo scambio di dati tra gli ambienti HQ e BR.
- Processi di Trasformazione dei Dati:** I processi coinvolti nella traduzione e sincronizzazione dei dati tra i sistemi ERP-HQ e ERP-BR, compresi eventuali logici implementati all'interno del middleware per garantire la compatibilità e la coerenza tra le due piattaforme ERP.

**Task****Descrizione**

**TASK P-12 Information Types**  
Identify the types of information to be processed, stored, and transmitted by the system.

**Nel contesto del sistema di integrazione middleware descritto nell'azienda, i tipi di informazioni da elaborare, archiviare e trasmettere includono:**

- **Dati Aziendali:** Questi dati comprendono informazioni relative alle vendite, agli acquisti, alla gestione del magazzino, alla finanza e alla contabilità. Sono informazioni critiche per il funzionamento dell'azienda e vengono trasferite tra l'ERP-HQ e l'ERP-BR attraverso il middleware.
- **Record dei Clienti:** Informazioni sui clienti, come dettagli di contatto, storico degli ordini e preferenze di acquisto, potrebbero essere elaborati, archiviati e trasmessi per garantire un servizio clienti efficiente e personalizzato.
- **Informazioni sugli Ordini:** Dati relativi agli ordini dei clienti, compresi prodotti acquistati, quantità, prezzi e dettagli di spedizione, devono essere elaborati per garantire la corretta gestione degli ordini e la consegna tempestiva dei prodotti.
- **Dati degli Utenti:** Informazioni sugli utenti autorizzati ad accedere ai sistemi ERP, compresi nomi utente, password e ruoli, devono essere elaborati, archiviati e trasmessi per garantire la sicurezza e l'accesso autorizzato al sistema.
- **Dati di Magazzino:** Informazioni sullo stock di merci, inclusi quantità disponibili, ubicazioni di magazzino e movimenti di inventario, devono essere elaborati per garantire una corretta gestione del magazzino e una pianificazione efficiente della produzione.
- **Dati di Produzione:** Informazioni sui processi di produzione, comprese linee di produzione, tempi di attività e resoconti di produzione, possono essere elaborati, archiviati e trasmessi per monitorare e ottimizzare l'efficienza della produzione.
- **Dati Finanziari:** Informazioni finanziarie, come bilanci contabili, flussi di cassa e report finanziari, devono essere elaborati per garantire una corretta gestione finanziaria e la conformità normativa.

**Task****Descrizione**

**TASK P-13 Information Life Cycle** Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system.

**Nel contesto dell'organizzazione e del sistema di integrazione descritto, identificare e comprendere tutte le fasi del ciclo di vita dell'informazione per ciascun tipo di informazione elaborata, archiviata o trasmessa dal sistema è fondamentale per una gestione efficace del rischio e per garantire la sicurezza delle informazioni.**

- **Elaborazione dell'Informazione:** Questa fase comprende tutte le attività coinvolte nell'acquisizione, nell'elaborazione e nella trasformazione dei dati da parte del middleware. Ciò include la traduzione dei record dall'ERP-HQ all'ERP-BR e viceversa mediante il modulo Convert, nonché le operazioni di lettura e scrittura dei dati nei database interni.
- **Archiviazione dell'Informazione:** I dati elaborati dal sistema di integrazione vengono archiviati nel database interno, che contiene le tabelle ERP-HQ e ERP-BR. È importante comprendere come vengono archiviati i dati, quali misure di sicurezza sono in atto per proteggere l'accesso non autorizzato e come vengono gestiti i backup e il ripristino dei dati.
- **Trasmissione dell'Informazione:** Durante la sincronizzazione dei dati tra l'ERP-HQ e l'ERP-BR, l'informazione viene trasmessa attraverso il middleware. È essenziale comprendere i protocolli di comunicazione utilizzati, le misure di sicurezza implementate per proteggere la trasmissione dei dati e come vengono gestite eventuali interruzioni o perdite di connessione.
- **Disposizione dell'Informazione:** Alla fine del ciclo di vita dell'informazione, potrebbe essere necessario disporre dei dati in modo sicuro e conforme alle normative. Ciò potrebbe includere la cancellazione sicura dei dati archiviati nel database interno quando non sono più necessari o la gestione delle informazioni obsolete in conformità con le politiche aziendali e normative applicabili.

**Task****Descrizione**

**TASK P-16 Enterprise Architecture Determine the placement of the system within the enterprise architecture.**

**Nel contesto dell'architettura aziendale, la collocazione del sistema di integrazione tra ERP-HQ e ERP-BR è un elemento cruciale da considerare. Ecco alcuni punti da tenere in considerazione per determinare la posizione ottimale del sistema all'interno dell'architettura aziendale:**

- **Integrazione con l'ERP-HQ e l'ERP-BR:** Il sistema di integrazione deve essere posizionato in modo tale da facilitare la comunicazione e lo scambio di dati tra l'ERP-HQ (situato presso la sede centrale) e l'ERP-BR (situato presso la filiale). Questo può implicare l'installazione del middleware su un server che sia facilmente accessibile da entrambi i sistemi ERP.
- **Localizzazione dei Dati e dei Flussi di Lavoro:** È importante considerare la localizzazione geografica dei dati e dei flussi di lavoro all'interno dell'azienda. Se l'ERP-HQ e l'ERP-BR sono situati in luoghi fisicamente distanti, potrebbe essere necessario implementare il sistema di integrazione in modo distribuito per ottimizzare le prestazioni e la latenza dei dati.
- **Architettura Cloud o On-Premise:** Data la natura critica del sistema di integrazione e la sua dipendenza da ERP-HQ e ERP-BR, potrebbe essere opportuno valutare l'implementazione del sistema su un'infrastruttura cloud o on-premise. La scelta dipenderà dalle esigenze di sicurezza, scalabilità, flessibilità e costi dell'organizzazione.
- **Accessibilità e Affidabilità:** È importante assicurarsi che il sistema di integrazione sia facilmente accessibile e altamente affidabile per garantire la continuità operativa e la sincronizzazione continua dei dati tra i due sistemi ERP. Questo potrebbe implicare l'implementazione di misure di ridondanza, backup e ripristino.
- **Conformità Normativa e Sicurezza:** Considerare i requisiti normativi e di sicurezza dell'azienda e assicurarsi che il sistema di integrazione sia conforme a tali normative e offra le necessarie misure di protezione dei dati, crittografia e monitoraggio delle attività.

# Raccomandazione finale

## Considerazioni:

- Costi e risorse: La soluzione SaaS/iPaaS riduce i costi iniziali e i tempi di manutenzione, consentendo di utilizzare le risorse interne in modo più efficiente.
- Sicurezza e conformità: SaaS/iPaaS offre robusti controlli di sicurezza gestiti dal provider, riducendo l'onere della gestione interna e garantendo una conformità continua.
- Scalabilità e flessibilità: La soluzione SaaS/iPaaS offre maggiore flessibilità e scalabilità, adattandosi meglio alle esigenze aziendali in evoluzione.

In base all'analisi svolta utilizzando il framework NIST SP 800-37r2 RMF, si raccomanda di sostituire il middleware on-premises con una soluzione SaaS/iPaaS. Questa opzione supporta meglio la strategia di gestione del rischio dell'organizzazione, allineandosi con gli obiettivi aziendali e garantendo una maggiore sicurezza e continuità operativa.

# Progetto S4/L2



## Gestione del rischio informatico per un caso aziendale specifico - Prepare e Categorize



## Prepare

Dopo aver completato i task dell'esercizio di ieri, oggi continueremo il progetto ultimando la fase Prepare e proseguendo con Categorize. Definite quali framework l'organizzazione intende usare ed effettuate un risk assessment solamente a livello sistema (l'estensione a livello organizzativo è un'estensione, TASK P-3):

- Identificare il rischio rispetto agli asset identificati ieri.
- Valutare il rischio; potete usare qualsiasi metodo.

Non inserite tutti i rischi con la stessa data, ma scegliete un arco temporale, così da ottenere dei grafici in cui si possa vedere una variazione nel tempo. Domani effettueremo il trattamento.

Nota: il risk assessment è ciclico, non è richiesta l'identificazione di tutti i rischi nella prima iterazione.

## Categorize

Produrre un piccolo documento che descriva le due architetture (raccogliete il materiale prodotto ieri), utilizzare SimpleRisk per la conservazione documentale tracciata (TASK C-1).

Task	Descrizione
<b>TASK P-4 Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles (Optional)</b> Establish, document, and publish organizationally-tailored control baselines and/or Cybersecurity Framework Profiles.	<p><b>Elenco dei Baseline di Controllo Organizzativamente Personalizzati Approvati o Diretti:</b></p> <ul style="list-style-type: none"> <li><b>Controllo degli Accessi (AC):</b> Implementazione di controlli di accesso basati sui ruoli (RBAC) per l'accesso ai dati all'interno della piattaforma di integrazione.</li> <li><b>Audit e Responsabilità (AU):</b> Registrazione e monitoraggio regolari delle transazioni di dati tra i sistemi ERP.</li> <li><b>Protezione dei Sistemi e delle Comunicazioni (SC):</b> Utilizzo di protocolli di comunicazione sicuri (ad esempio, TLS) per la trasmissione dei dati.</li> <li><b>Integrità dei Sistemi e delle Informazioni (SI):</b> Aggiornamenti regolari e gestione delle patch della piattaforma SaaS/iPaaS per affrontare le vulnerabilità.</li> </ul>
<b>TASK P-14 Risk Assessment—System</b> Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.	<p><b>Sulla base dei rischi identificati, vengono selezionati i seguenti controlli di sicurezza:</b></p> <ul style="list-style-type: none"> <li><b>Crittografia:</b> Utilizzare la crittografia AES-256 per i dati a riposo e TLS 1.2 per i dati in transito.</li> <li><b>Gestione degli accessi:</b> Implementare Azure Active Directory e RBAC.</li> <li><b>Gestione della conformità:</b> Garantire il rispetto del GDPR, dell'HIPAA e di altre normative pertinenti.</li> <li><b>Gestione della disponibilità:</b> Utilizzare i servizi supportati da SLA di Azure per un'elevata disponibilità e per il ripristino in caso di disastri.</li> <li><b>Verifiche dell'integrità dei dati:</b> Implementare checksum e meccanismi di convalida dei dati all'interno delle pipeline dei dati.</li> </ul>

**Task****Descrizione**

**TASK C-1 System Description**  
Document the characteristics  
of the system.

**Servizio Data Factory:**

- **Pipeline dei dati:** Creare e gestire flussi di lavoro basati sui dati. Le pipeline dei dati sposteranno i dati tra ERP-HQ e ERP-BR, eseguendo le trasformazioni necessarie.
- **Flussi di dati di mappatura:** Interfaccia low-code/no-code per la trasformazione dei dati. Questo sostituirà il modulo Convert, traducendo i record dai formati di ERP-HQ a ERP-BR e viceversa.

**Runtime di integrazione:**

- **Runtime di integrazione ospitato in Azure:** Gestisce le attività di spostamento e trasformazione dei dati nel cloud.
- **Runtime di integrazione self-hosted:** Si connette a ERP-HQ on-premises e a ERP-BR ospitato nel cloud per trasferimenti dati sicuri ed efficienti.

**Archiviazione e calcolo:**

- **Database SQL di Azure:** Utilizzato per lo storage dei dati intermedi durante le trasformazioni.
- **Archiviazione Blob di Azure:** Archiviazione dei dati grezzi e dei log per audit e risoluzione dei problemi.

**Monitoraggio e gestione:**

- **Azure Monitor:** Fornisce monitoraggio e segnalazioni in tempo reale per le attività di Data Factory.
- **Azure Security Center:** Garantisce la conformità agli standard di sicurezza e alle migliori pratiche.

**Sicurezza:**

- **Crittografia:** I dati a riposo e in transito saranno crittografati utilizzando i meccanismi di crittografia integrati di Azure.
- **Controllo degli accessi:** Controllo degli accessi basato sui ruoli (RBAC) per gestire le autorizzazioni e garantire che solo il personale autorizzato possa accedere e gestire i flussi di integrazione.
- **Conformità:** Adesione alle linee guida NIST SP 800-37r2 RMF per migliorare la postura della sicurezza.

# Asset



Governance La Gestione Del Rischio Conformità Asset Management Valutazioni Reporting Configurare

Q ? - Angelo Di Mauro -

- 1 La Scoperta Automatica
  - 2 La Gestione Di Attività
  - 3 Gestire i gruppi di risorse

+ | Gruppi di risorse (2)

Nome	Indirizzo IP	Per La Valutazione Delle Attività	Sito/Posizione	Squadra	Dettagli di asset	Tag	
# Cloud - TIER 2							<input checked="" type="checkbox"/> <input type="checkbox"/>
ERP-BR	N/A	\$100,001 to \$200,000	Cloud				<input type="checkbox"/>
# Data-center - TIER 1							<input checked="" type="checkbox"/> <input type="checkbox"/>
DB	N/A	\$100,001 to \$200,000	on-premises				<input type="checkbox"/>
ERP-HQ	N/A	\$400,001 to \$500,000	on-premises				<input type="checkbox"/>
Middleware	N/A	\$0 to \$100,000	on-premises				<input type="checkbox"/>

Page 1 of

Displaying 1 to 2 of 2 items

Quadri

Controlli

1 Definire quadri di controllo

2 Programma del documento

3 Definizione delle eccezioni



Framework attivi (2)

Strutture inattive (0)

Nome del Framework	Framework Descrizione	
NIST CSF		<input checked="" type="checkbox"/> <input type="checkbox"/>
NIST 800-53		<input checked="" type="checkbox"/> <input type="checkbox"/>

# Framework & Rischi

Elenco dei r...

1 Invia Rischio

2 Piano di mitigazione

3 Eseguire recensioni

4 Progetti di piano

5 Esaminare regolarmente

Di seguito è riportato l'elenco delle domande di rischi che richiedono la strategia di mitigazione.

ID	Stato	Soggetto	Inherent Risk (Current)	Data Di Presentazione	Mitigazione Prevista	Riesame Della Direzione
1005	New	TASK P-14 / Interruzione del servizio	6	05/20/2024 5:31 AM CDT	NO	NO
1006	New	TASK P-14 / Data Breach	3.2	05/20/2024 5:43 AM CDT	NO	NO

# Progetto S4/L3



## Gestione del rischio informatico per un caso aziendale specifico - Select e Implement



## Select

Nella fase Select, selezionerete quali controlli utilizzare per i vostri due sistemi. Se necessario, potete adattare i controlli al vostro scenario (TASK S-2). Poi, allocate i vari controlli sulle componenti del sistema, facendo ad esempio una tabella Excel di mapping controllo/asset (TASK S-3) e documentate le decisioni prese (TASK S-4). Inserite nel documento anche la strategia che utilizzerete per monitorare l'efficacia dei controlli (TASK S-5). Nella selezione dei controlli, includete una stima del costo del controllo. Ricordate che non dovete per forza selezionare dei controlli, potete utilizzare altre tipologie di trattamento (es. accettazione).

## Implement

Implementate i controlli in SimpleRisk (TASK I-1), effettuando così una mitigazione del rischio e ottenendo dei valori di rischio residuo. Non concentrate tutti i controlli nello stesso giorno, ma utilizzate un arco temporale, così da ottenere dei grafici in cui si possa vedere una variazione nel tempo. In questa fase, la risposta al rischio non è ancora stata sottoposta alla direzione per l'approvazione (non fate clic su "Accept Mitigation" in Risk/Mitigation).

Task	Descrizione
TASK S-1 Control Selection Select the controls for the system and the environment of operation.	<p><b>Controlli di Accesso:</b></p> <ul style="list-style-type: none"> <li>○ <b>Implementazione di autenticazione a più fattori per gli utenti autorizzati ad accedere alla soluzione Azure Data Factory.</b></li> <li>○ <b>Definizione di ruoli e autorizzazioni per limitare l'accesso solo alle risorse e funzionalità necessarie.</b></li> <li>○ <b>Monitoraggio e registrazione degli accessi per l'audit e la rilevazione di comportamenti anomali.</b></li> </ul> <p><b>Controlli di Crittografia:</b></p> <ul style="list-style-type: none"> <li>○ <b>Utilizzo di crittografia per proteggere i dati in transito tra la soluzione Azure Data Factory e gli ERP HQ e BR.</b></li> <li>○ <b>Crittografia dei dati sensibili durante la memorizzazione nel cloud per garantirne la riservatezza.</b></li> </ul> <p><b>Controlli di Monitoraggio e Registrazione:</b></p> <ul style="list-style-type: none"> <li>○ <b>Configurazione di registri di controllo per monitorare l'attività del sistema, inclusi gli accessi, le modifiche ai dati e le operazioni di trasformazione.</b></li> <li>○ <b>Implementazione di sistemi di monitoraggio continuo per rilevare e rispondere prontamente a potenziali minacce o violazioni della sicurezza.</b></li> </ul> <p><b>Controlli di Conformità:</b></p> <ul style="list-style-type: none"> <li>○ <b>Adozione di procedure e controlli per garantire la conformità alle normative pertinenti come GDPR, HIPAA, o altre regolamentazioni settoriali.</b></li> <li>○ <b>Verifica periodica della conformità e delle politiche di sicurezza per garantire che il sistema soddisfi costantemente gli standard richiesti.</b></li> </ul> <p><b>Controlli di Risposta agli Incidenti:</b></p> <ul style="list-style-type: none"> <li>○ <b>Sviluppo di un piano di risposta agli incidenti che definisce i processi e le procedure da seguire in caso di violazione della sicurezza o incidente informatico.</b></li> <li>○ <b>Esecuzione di esercitazioni periodiche di risposta agli incidenti per testare l'efficacia del piano e identificare eventuali aree di miglioramento.</b></li> </ul> <p><b>Controlli di Gestione degli Accessi Privilegiati:</b></p> <ul style="list-style-type: none"> <li>○ <b>Limitazione dell'accesso privilegiato solo a utenti autorizzati e necessari per l'amministrazione e la gestione della soluzione Azure Data Factory.</b></li> <li>○ <b>Implementazione di monitoraggio e registrazione specifici per le attività degli amministratori per garantire la tracciabilità delle azioni privilegiate.</b></li> </ul>

**Task****Descrizione**

**TASK S-2  
Control  
Tailoring Tailor  
the controls  
selected for the  
system and the  
environment of  
operation.**

- Controllo dell'Accesso ai Dati:**
- **Implementazione di controlli per garantire che solo gli utenti autorizzati possano accedere ai dati sensibili e alle risorse del sistema Azure Data Factory.**
  - **Definizione di politiche di accesso basate su ruoli per limitare l'accesso solo alle funzionalità e ai dati necessari per l'esecuzione delle attività.**
- Monitoraggio delle Attività del Sistema:**
- **Configurazione di strumenti di monitoraggio per rilevare e registrare le attività del sistema, inclusi gli accessi degli utenti, le operazioni di trasformazione dei dati e gli eventi di sistema.**
  - **Analisi periodica dei log di attività per identificare comportamenti anomali o potenziali minacce alla sicurezza.**
- Backup e Ripristino dei Dati:**
- **Implementazione di procedure di backup regolari per garantire la disponibilità e l'integrità dei dati gestiti dalla soluzione Azure Data Factory.**
  - **Verifica periodica dei processi di backup e ripristino per assicurare che siano in grado di ripristinare i dati in caso di perdita o corruzione.**
- Gestione delle Patch e degli Aggiornamenti:**
- **Monitoraggio costante per identificare e applicare tempestivamente patch di sicurezza e aggiornamenti del sistema operativo e del software della soluzione Azure Data Factory.**
  - **Pianificazione regolare di manutenzione preventiva per garantire che il sistema sia protetto contro le vulnerabilità note.**
- Gestione dei Rischi:**
- **Conduzione di valutazioni dei rischi periodiche per identificare e valutare le minacce alla sicurezza e le vulnerabilità del sistema.**
  - **Implementazione di misure di mitigazione dei rischi per ridurre l'impatto di potenziali minacce e vulnerabilità identificate.**
- Formazione e Consapevolezza degli Utenti:**
- **Fornitura di formazione sulla sicurezza informatica per educare gli utenti sull'importanza delle pratiche sicure e per ridurre il rischio di violazioni della sicurezza dovute a errori umani.**
  - **Promozione di una cultura della sicurezza informatica all'interno dell'organizzazione per aumentare la consapevolezza e la prontezza alla sicurezza.**

Task	Descrizione
TASK S-3 Control Allocation Allocate security and privacy controls to the system and to the environment of operation.	<p><b>Controlli di Sicurezza e Privacy Assegnati al Sistema e all'Ambiente di Operazione</b></p> <p><b>Controllo degli Accessi:</b></p> <ul style="list-style-type: none"> <li>○ Definizione di politiche di accesso e autorizzazioni per garantire che solo gli utenti autorizzati possano accedere alle risorse del sistema.</li> <li>○ Implementazione di meccanismi di autenticazione multi-fattore per aumentare la sicurezza dell'accesso.</li> <li>○ Assegnazione di ruoli e privilegi appropriati agli utenti in base alle loro responsabilità.</li> </ul> <p><b>Protezione dei Dati:</b></p> <ul style="list-style-type: none"> <li>○ Implementazione di crittografia per proteggere i dati sensibili durante la trasmissione e la memorizzazione.</li> <li>○ Definizione di politiche per garantire la riservatezza, l'integrità e la disponibilità dei dati.</li> </ul> <p><b>Monitoraggio e Registrazione delle Attività:</b></p> <ul style="list-style-type: none"> <li>○ Configurazione di strumenti di monitoraggio per rilevare e registrare le attività del sistema e degli utenti.</li> <li>○ Analisi periodica dei log di sicurezza per identificare e rispondere prontamente agli eventi di sicurezza.</li> </ul> <p><b>Gestione degli Aggiornamenti e delle Patch:</b></p> <ul style="list-style-type: none"> <li>○ Pianificazione e applicazione regolare di patch di sicurezza per proteggere il sistema da vulnerabilità note.</li> <li>○ Verifica della compatibilità e del corretto funzionamento delle patch prima dell'applicazione.</li> </ul> <p><b>Gestione dei Rischi:</b></p> <ul style="list-style-type: none"> <li>○ Identificazione e valutazione periodica dei rischi per il sistema e l'ambiente di operazione.</li> <li>○ Implementazione di misure di mitigazione per ridurre l'impatto dei rischi identificati.</li> </ul> <p><b>Formazione e Consapevolezza degli Utenti:</b></p> <ul style="list-style-type: none"> <li>○ Fornitura di formazione sulla sicurezza informatica per sensibilizzare gli utenti sull'importanza delle pratiche sicure.</li> <li>○ Promozione di una cultura della sicurezza informatica per ridurre il rischio di violazioni della sicurezza dovute a errori umani.</li> </ul>

**Task****Descrizione**

**TASK S-4**  
**Documentation of Planned Control Implementations**  
Document the controls for the system and environment of operation in security and privacy plans.

### **Piani di Sicurezza e Privacy per il Sistema**

I piani di sicurezza e privacy per il sistema Azure Data Factory saranno sviluppati considerando una serie di fattori, inclusi i risultati dell'analisi dei rischi, i requisiti di sicurezza e privacy, nonché le politiche e le strategie organizzative pertinenti. I controlli selezionati per il sistema e l'ambiente di operazione saranno integrati in questi piani per garantire la sicurezza e la protezione dei dati gestiti dalla soluzione.

#### **Categorizzazione della Sicurezza:**

- Definizione della categorizzazione della sicurezza per identificare e classificare i dati e le risorse del sistema in base al loro valore e alla sensibilità.

#### **Analisi dei Rischi:**

- Utilizzo dei risultati dell'analisi dei rischi per identificare e valutare le minacce e le vulnerabilità del sistema, nonché per determinare le misure di mitigazione necessarie.

#### **Requisiti di Sicurezza e Privacy:**

- Elaborazione di requisiti dettagliati di sicurezza e privacy per il sistema, inclusi requisiti specifici per gli elementi di sistema e l'ambiente di operazione.

#### **Strategia di Gestione dei Rischi:**

- Definizione di una strategia di gestione dei rischi che delinei le attività e le responsabilità per il monitoraggio e la gestione dei rischi nel tempo.

#### **Controlli Selezionati:**

- Implementazione dei controlli selezionati per il sistema e l'ambiente di operazione, compresi i controlli di accesso, crittografia, monitoraggio e risposta agli incidenti.

#### **Politiche Organizzative:**

- Incorporazione delle politiche organizzative di sicurezza, privacy e gestione della catena di fornitura nei piani di sicurezza e privacy per il sistema.

Task	Descrizione
TASK I-1 Control Implementation Implement the controls in the security and privacy plans.	<p><b>Mitigazione del Rischio</b></p> <ol style="list-style-type: none"> <li><b>1. Valutazione del Rischio Iniziale</b> <ul style="list-style-type: none"> <li>• <b>Identificazione del Rischio:</b> Identificare i rischi associati ai processi aziendali, alle informazioni e ai sistemi.</li> <li>• <b>Valutazione:</b> Valutare il livello di rischio (probabilità e impatto) prima dell'implementazione dei controlli.</li> </ul> </li> <li><b>2. Implementazione dei Controlli di Mitigazione</b> <ul style="list-style-type: none"> <li>• <b>Selezione dei Controlli:</b> Selezionare i controlli appropriati per mitigare i rischi identificati.</li> <li>• <b>Implementazione:</b> Seguire il processo dettagliato di implementazione dei controlli descritto sopra.</li> </ul> </li> <li><b>3. Valutazione del Rischio Residuo</b> <ul style="list-style-type: none"> <li>• <b>Rivalutazione:</b> Dopo l'implementazione dei controlli, rivalutare i rischi per determinare il livello di rischio residuo.</li> <li>• <b>Metodi di Valutazione:</b> Utilizzare metodologie quantitative e qualitative per misurare l'efficacia dei controlli e il livello di rischio residuo.</li> </ul> </li> <li><b>4. Azioni Correttive</b> <ul style="list-style-type: none"> <li>• <b>Analisi del Rischio Residuo:</b> Se il rischio residuo è ancora troppo elevato, identificare ulteriori azioni correttive.</li> <li>• <b>Piani di Miglioramento:</b> Sviluppare e implementare piani di miglioramento per ridurre ulteriormente il rischio residuo.</li> <li>• <b>Documentazione:</b> Documentare tutte le azioni correttive intraprese e i risultati ottenuti.</li> </ul> </li> <li><b>5. Monitoraggio Continuo</b> <ul style="list-style-type: none"> <li>• <b>Revisione Periodica:</b> Effettuare revisioni periodiche del rischio e dei controlli per assicurarsi che rimangano efficaci e appropriati.</li> <li>• <b>Aggiornamenti:</b> Aggiornare la valutazione del rischio e i controlli in risposta a nuove minacce, vulnerabilità e cambiamenti nell'ambiente aziendale.</li> </ul> </li> </ol>

# Rappresentazione grafica dei rischi e problemi



Governance La Gestione Del Rischio Conformità Asset Management Valutazioni Reporting Configurare

Q ? Angelo Di Mauro

- Panoramica
- Rischio Dashboard
- Rischi e problemi
- Rapporto sull'appetito di rischio
- Rischio Di Tendenza
- Rapporto di rischio dinamico
- Analisi grafica del rischio
- Visualizzatore di connettività
- Media di rischio nel tempo
- Probabilità e impatto
- Consigli Di Rischio
- Rischi e Attività
- Rischi e controlli
- Tutti aperti rischi assegnati a Me
- Tutti Aperti i Rischi che Necessitano di una Revisione
- Tutti i rischi dal Team di livello di rischio
- Ad Alto Rischio Di Report
- Inviato Rischi Per Data

Tag di rischio:  None selected

Data di inizio:  04/21/2024

Data di fine:  05/21/2024

Tendenza : Crescente ↑ ; Decrescente ↓ ; Nessun cambiamento ↔ ;

Stato :  (Very High);  (High);  (Medium);  (Low);  (Insignificante);

Categoria	Stato	Tendenza	Dettagli
Technical Vulnerability Management		↔	<b>1005 : TASK P-14 / Interruzione del servizio</b>
		↔	<b>1006 : TASK P-14 / Data Breach</b>

EXAMPLE

- 1 Invia Rischio
- 2 Piano di mitigazione
- 3 Eseguire recensioni
- 4 Progetti di piano
- 5 Esaminare regolarmente



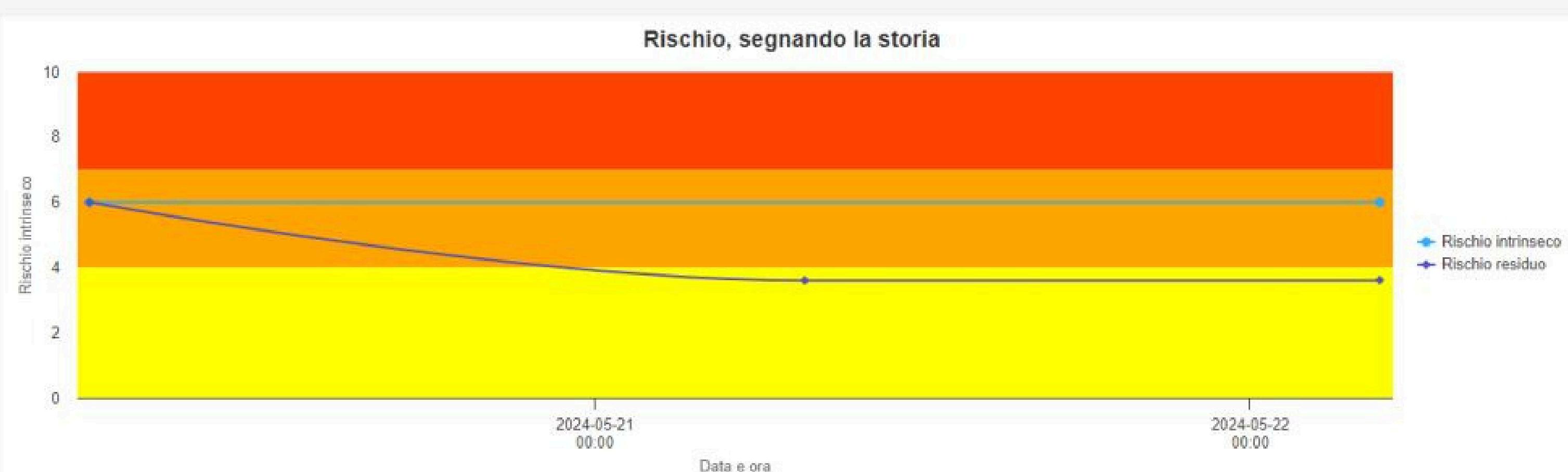
Id #: 1005

Stato: Mitigation Planned

Azioni

Subject: TASK P-14 / Interruzione del servizio [Edit](#)

- Vedi rischio segnando dettagli  
▼ Nascondere il Punteggio di rischio nel tempo

[Reimposta mitigazioni](#)

- 1 Invia Rischio
- 2 Piano di mitigazione
- 3 Eseguire recensioni
- 4 Progetti di piano
- 5 Esaminare regolarmente

Rischio  
intrinseco  
**3.2**  
Low

Rischio residuo  
**0.96**  
Low

Id #: 1006

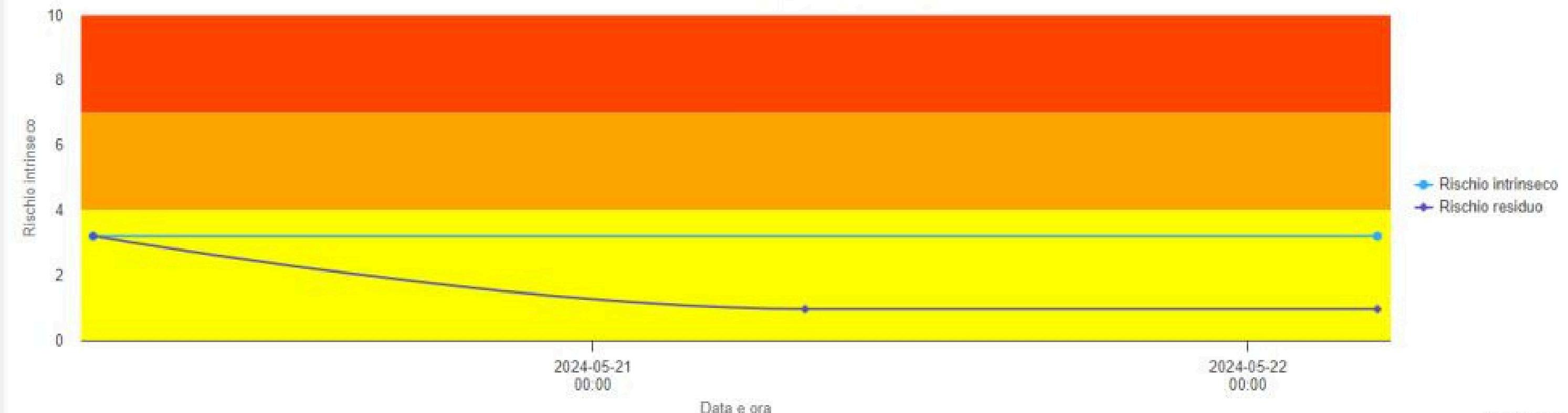
Stato: Mitigation Planned

Azione

Subject: TASK P-14 / Data Breach 

- ▶ Vedi rischio segnando dettagli  
▼ Nascondere il Punteggio di rischio nel tempo

### Rischio, segnando la storia



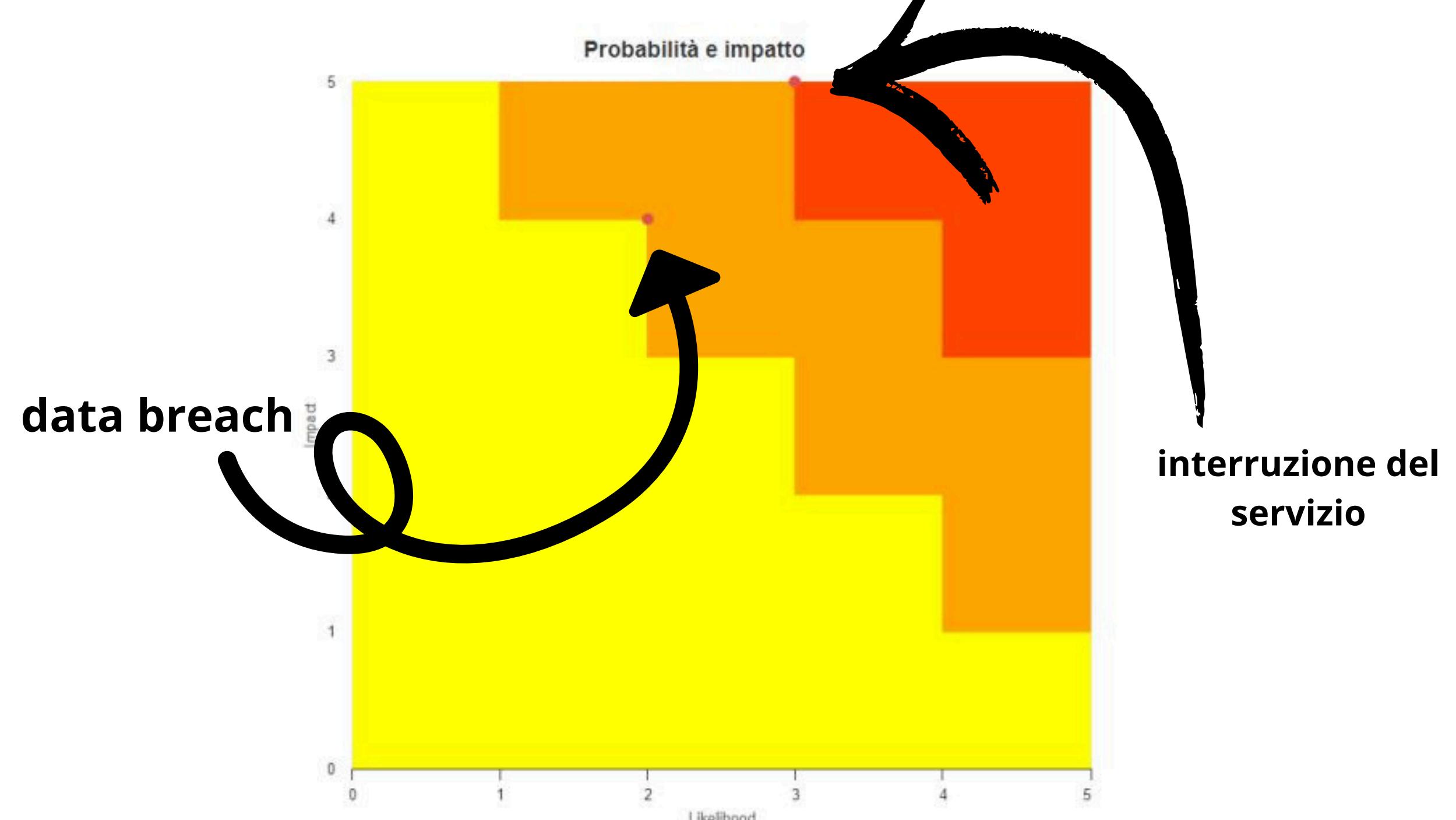
Highcharts.com

[Dettagli](#) [Di mitigazione](#) [Recensione](#)[Modifica Dettagli](#)

Mappatura dei rischi: Privilege escalation, Unauthorized access, Loss of integrity through unauthorized changes

Mappatura delle minacce: Hacking &amp; Other Cybersecurity Crimes

-  Panoramica
-  Rischio Dashboard
-  Rischi e problemi
-  Rapporto sull'appetito di rischio
-  Rischio Di Tendenza
-  Rapporto di rischio dinamico
-  Analisi grafica del rischio
-  Visualizzatore di connettività
-  Media di rischio nel tempo
-  Probabilità e impatto
-  Consigli Di Rischio
-  Rischi e Attività
-  Rischi e controlli
-  Tutti aperti rischi assegnati a Me
-  Tutti Aperti i Rischi che Necessitano di una Revisione
-  Tutti i rischi dal Team di livello di rischio
-  Ad Alto Rischio Di Report
-  Inviato Rischi Per Data



# Piano di Mitigazione del Rischio

Risk list ID: 1006 TASK P-1...

1 Invia Rischio  
2 Piano di mitigazione  
**3 Eseguire recensioni**  
4 Progetti di piano  
5 Esaminare regolarmente

Rischio intrinseco: 3.2 Low | Rischio residuo: 0.96 Low

Id #: 1006 Stato: Mitigation Planned Subject: TASK P-14 / Data Breach [Edit](#)

Dettagli Di mitigazione Recensione Modifica Di Mitigazione

Data di presentazione di: 05/21/2024 Soluzione Corrente: trasferiamo il nostro rischio ad un provider di Cloud Saas

mitigazione:

Data di mitigazione prevista: 05/21/2024 Requisiti Di Sicurezza: Autenticazione, autorizzazione, integrità

Strategia Di Pianificazione: Transfer Raccomandazioni Per La Sicurezza:

Sforzo Di Mitigazione: Significant La Documentazione Di Supporto: Nessuno

Riduzione Dei Costi: \$100,001 to \$200,000

Di Mitigazione Del Proprietario: Angelo Di Mauro

Di Mitigazione Del Team: Data Center & Storage, Database

Per cento di mitigazione: 70%

[Accetta attenuazione](#)

▶ Commenti

- Panoramica
- Rischio Dashboard
- Rischi e problemi
- Rapporto sull'appetito di rischio**
- Rischio Di Tendenza
- Rapporto di rischio dinamico
- Analisi grafica del rischio
- Visualizzatore di connettività
- Media di rischio nel tempo
- Probabilità e impatto
- Consigli Di Rischio
- Rischi e Attività
- Rischi e controlli
- Tutti aperti rischi assegnati a Me
- Tutti Aperti i Rischi che Necessitano di una Revisione
- Tutti i rischi dal Team di livello di rischio
- Ad Alto Rischio Di Report
- Inviato Rischio Per Data

Questo report visualizza tutte le attenuazioni previste ordinate per data di mitigazione.

ID	Soggetto	Data di presentazione di mitigazione	Strategia Di Pianificazione	Sforzo Di Mitigazione	Riduzione Dei Costi	Di Mitigazione Del Proprietario	Di Mitigazione Del Team	Inviato Da
ID	Soggetto	Data di presenta	Strategia Di Pian	Sforzo Di Mitig	Riduzione Del C	Di Mitigazione D	Di Mitigazione Del Team	Inviato Da
1006	TASK P-14 / Data Breach	05/21/2024 07:47	Transfer	Significant	\$100,001 to \$200,000	Angelo Di Mauro	Data Center & Storage,Database	Angelo Di Mauro
1005	TASK P-14 / Interruzione del servizio	05/21/2024 07:43	Mitigate	Considerable	\$100,001 to \$200,000	Angelo Di Mauro	Data Center & Storage,Database,IT Systems Management,Network/Web Systems	Angelo Di Mauro

Showing 1 to 2 of 2 entries

**La mitigazione del rischio riguarda le azioni intraprese per ridurre la probabilità o l'impatto di un rischio. Si tratta di implementare misure preventive, come migliorare la sicurezza, formare il personale o aggiornare le infrastrutture, per evitare che il rischio si concretizzi o per limitarne le conseguenze negative.**

**Il trasferimento del rischio, invece, consiste nel spostare la responsabilità finanziaria e le conseguenze del rischio a una terza parte, solitamente attraverso assicurazioni o contratti. Ad esempio, acquistare una polizza assicurativa o esternalizzare servizi a fornitori esterni, in modo che siano loro a gestire i rischi associati.**

# Previsioni di mitigazione

- Panoramica
- Rischio Dashboard
- Rischi e problemi
- Rapporto sull'appetito di rischio
- Rischio Di Tendenza
- Rapporto di rischio dinamico
- Analisi grafica del rischio
- Visualizzatore di connettività
- Media di rischio nel tempo
- Probabilità e impatto
- Consigli Di Rischio
- Rischi e Attività
- Rischi e controlli
- Tutti aperti rischi assegnati a Me
- Tutti Aperti i Rischi che Necessitano di una Revisione
- Tutti i rischi dal Team di livello di rischio
- Ad Alto Rischio Di Report
- Inviato Rischii Per Data
- Strategie Di Riduzione Del Rischio Per Data
- Gestione Del Cliente Dalla Data Di

Tag di rischio:  Data di inizio:  Data di fine:

Tendenza : Crescente ↑ ; Decrescente ↓ ; Nessun cambiamento ↔ ;

Stato : ■ (Very High); ■ (High); ■ (Medium); ■ (Low); □ (Insignificante);

Categoria	Stato	Tendenza	Dettagli
Technical Vulnerability Management	Low	↓	<b>1005 : TASK P-14 / Interruzione del servizio</b>
	Low	↓	<b>1006 : TASK P-14 / Data Breach</b>

# Progetto S4/L4



## Gestione del rischio informatico per un caso aziendale specifico - Assessment



**Task****Descrizione**

**TASK A-1**  
**Assessor Selection**  
Select the appropriate assessor or assessment team for the type of control assessment to be conducted.

**Obiettivi:**

- **Identificazione delle Competenze Necessarie:** Determinare le competenze tecniche e organizzative richieste.
- **Selezione dei Membri del Team:** Identificare membri con esperienze complementari in sicurezza informatica, gestione IT, conformità normativa e valutazione dei rischi.
- **Assegnazione dei Ruoli:** Definire ruoli e responsabilità di ciascun membro.
- **Comunicazione e Pianificazione:** Organizzare una riunione preliminare per discutere obiettivi, metodi e piano di lavoro.

**Output del Task A-1:**

- **Team Costituito:** Gruppo di esperti selezionato e informato sui rispettivi ruoli.
- **Piano di Comunicazione:** Stabilito un piano di comunicazione efficace.
- **Riunione Preliminare:** Discussione del piano di lavoro e metodi di assessment completata.

**Task****Descrizione**

<p><b>TASK A-2</b> <b>Assessment Plan</b> Develop, review, and approve plans to assess implemented controls.</p>	<p><b>Piano di Assessment dei Controlli di Sicurezza e Privacy</b></p> <p><b>Obiettivo:</b> Valutare l'efficacia e la conformità dei controlli di sicurezza e privacy nel sistema informativo aziendale.</p> <p><b>Componenti del Sistema da Valutare</b></p> <p><b>Server e Database:</b></p> <ul style="list-style-type: none"><li>• Controlli di accesso ai dati</li><li>• Sistemi di cifratura dei dati</li></ul> <p><b>Reti e Infrastrutture:</b></p> <ul style="list-style-type: none"><li>• Firewall e sistemi di rilevamento delle intrusioni</li><li>• Politiche di gestione delle vulnerabilità</li></ul> <p><b>Processi Operativi:</b></p> <ul style="list-style-type: none"><li>• Gestione delle patch e aggiornamenti software</li><li>• Procedure di risposta agli incidenti</li></ul> <p><b>Controlli da Valutare</b></p> <ul style="list-style-type: none"><li>• Controlli di Accesso:</li><li>• Autenticazione a due fattori</li><li>• Gestione delle credenziali</li></ul> <p><b>Controlli di Protezione dei Dati:</b></p> <ul style="list-style-type: none"><li>• Cifratura dei dati a riposo</li><li>• Backup e ripristino dei dati</li></ul> <p><b>Controlli di Rilevamento:</b></p> <ul style="list-style-type: none"><li>• Sistemi di logging e monitoraggio</li><li>• Analisi dei log di sicurezza</li></ul> <p><b>Controlli di Risposta e Ripristino:</b></p> <ul style="list-style-type: none"><li>• Piani di risposta agli incidenti</li><li>• Procedure di disaster recovery</li></ul> <p><b>Ispezioni Documentali:</b></p> <ul style="list-style-type: none"><li>• Policy di sicurezza</li><li>• Procedure operative standard (SOP)</li></ul> <p><b>Test Tecnici:</b></p> <ul style="list-style-type: none"><li>• Penetration testing</li><li>• Vulnerability scanning</li></ul> <p><b>Output del Task A-2:</b></p> <ul style="list-style-type: none"><li>• <b>Piano di Assessment Documentato:</b> Documento dettagliato che guida l'intero processo di assessment.</li><li>• <b>Calendario delle Attività:</b> Slot temporali specifici per ogni attività pianificata.</li><li>• <b>Distribuzione:</b> Piano condiviso e compreso da tutti i membri del team di assessment.</li></ul>
--	--

Task	Descrizione
<p><b>TASK A-3</b>  <b>Control</b>  <b>Assessments</b>  <b>Assess the</b>  <b>controls in</b>  <b>accordance with</b>  <b>the assessment</b>  <b>procedures</b>  <b>described in</b>  <b>assessment</b>  <b>plans.</b></p>	<p><b>Metodo di Assessment:</b></p> <ol style="list-style-type: none"> <li>1. <b>Interviste:</b> <ul style="list-style-type: none"> <li>○ <b>Obiettivo:</b> Raccogliere informazioni dettagliate sui processi e le implementazioni direttamente dai responsabili.</li> <li>○ <b>Partecipanti:</b> Responsabili IT, sviluppatori, e personale di sicurezza.</li> </ul> </li> <li>2. <b>Ispezioni Documentali:</b> <ul style="list-style-type: none"> <li>○ <b>Obiettivo:</b> Verificare l'esistenza e l'aggiornamento della documentazione relativa ai controlli di sicurezza.</li> <li>○ <b>Documenti da Esaminare:</b> <ul style="list-style-type: none"> <li>■ <b>Piano di contingenza e rapporti di test (CP-2)</b></li> <li>■ <b>Rapporti di scansione delle vulnerabilità (RA-5)</b></li> <li>■ <b>Politiche di accesso e log di audit (AC-3)</b></li> <li>■ <b>Risultati dei test di sicurezza del middleware (SA-11)</b></li> <li>■ <b>Documentazione dei meccanismi di protezione della trasmissione dei dati (SC-8)</b></li> </ul> </li> </ul> </li> </ol> <p><b>Procedura:</b></p> <ol style="list-style-type: none"> <li>1. <b>Preparazione:</b> <ul style="list-style-type: none"> <li>○ <b>Riunione Iniziale:</b> Breve incontro per coordinare le attività del team.</li> <li>○ <b>Distribuzione dei Compiti:</b> Assegnazione delle attività di intervista e ispezione documentale ai membri del team.</li> </ul> </li> <li>2. <b>Esecuzione:</b> <ul style="list-style-type: none"> <li>○ <b>Interviste:</b> Condurre interviste secondo l'elenco delle domande preparate.</li> <li>○ <b>Ispezioni Documentali:</b> Esaminare i documenti per verificare la conformità e l'efficacia dei controlli.</li> </ul> </li> <li>3. <b>Raccolta dei Dati:</b> <ul style="list-style-type: none"> <li>○ <b>Note e Osservazioni:</b> Annotare tutte le risposte delle interviste e le osservazioni fatte durante le ispezioni documentali.</li> <li>○ <b>Evidenze:</b> Raccogliere copie o estratti dei documenti esaminati come prove.</li> </ul> </li> </ol> <p><b>Output del Task A-3:</b></p> <ul style="list-style-type: none"> <li>• <b>Dati Raccolti:</b> Informazioni dettagliate sulle implementazioni dei controlli.</li> <li>• <b>Note e Osservazioni:</b> Documentazione delle interviste e ispezioni.</li> <li>• <b>Evidenze:</b> Prove documentali per supportare le valutazioni.</li> </ul>

Task	Descrizione
<b>TASK A-4</b> <b>Assessment Reports</b> Prepare the assessment reports documenting the findings and recommendations from the control assessments	<p><b>Obiettivo:</b> Documentare i risultati dell'assessment, valutando l'efficacia dei controlli di sicurezza.</p> <p><b>Attività:</b></p> <ol style="list-style-type: none"> <li>1. <b>Raccolta e Analisi Dati:</b> <ul style="list-style-type: none"> <li>○ Raccogliere note e evidenze dalle interviste e ispezioni.</li> <li>○ Analizzare i dati per valutare conformità e non conformità dei controlli.</li> </ul> </li> <li>2. <b>Preparazione del Report:</b> <ul style="list-style-type: none"> <li>○ Introduzione: Obiettivi e descrizione del sistema.</li> <li>○ Metodologia: Attività svolte.</li> <li>○ Risultati: Valutazione dei controlli specifici.</li> <li>○ Conclusioni: Sintesi dei risultati e raccomandazioni.</li> </ul> </li> <li>3. <b>Compilazione delle Risultanze:</b> <ul style="list-style-type: none"> <li>○ Conformità: Controlli correttamente implementati.</li> <li>○ Non Conformità: Controlli non adeguati.</li> <li>○ Raccomandazioni: Suggerimenti per miglioramenti.</li> <li>○ Osservazioni: Note aggiuntive.</li> </ul> </li> </ol> <p><b>Conclusione:</b> Produrre un report dettagliato per monitorare e gestire le azioni correttive, garantendo sicurezza e conformità del sistema.</p>

# Attività da svolgere

## **Identificazione delle Competenze Necessarie:**

- **Determinare le competenze tecniche e organizzative necessarie per l'assessment.**
- **Considerare competenze in sicurezza informatica, gestione IT, conformità normativa e valutazione dei rischi.**

## **Selezione dei Membri del Team:**

- **Identificare e selezionare i membri del team che possiedono le competenze necessarie.**
- **Garantire che il team sia composto da persone con esperienze diverse per coprire tutti gli aspetti della valutazione.**

## **Assegnazione dei Ruoli:**

- **Definire chiaramente i ruoli e le responsabilità di ciascun membro del team.**
- **Assicurarsi che ogni membro del team comprenda il proprio ruolo nell'assessment.**

## **Comunicazione e Pianificazione:**

- **Organizzare una riunione preliminare per discutere gli obiettivi dell'assessment, i metodi e il piano di lavoro.**
- **Stabilire un canale di comunicazione efficace tra i membri del team.**

# Il team di Assessment

## **Project Manager:**

**Nome: Alex Fiorillo**

**Responsabilità: Coordinare il processo di assessment, gestire pianificazione e comunicazione.**

## **Security Analyst:**

**Nome: Andrea Dura**

**Responsabilità: Condurre l'analisi delle vulnerabilità, valutare i controlli di sicurezza tecnica.**

## **IT Specialist:**

**Nome: Marco D' Antoni**

**Responsabilità: Verificare l'implementazione tecnica dei controlli, inclusi i test di sicurezza del middleware.**

## **Compliance Officer:**

**Nome: Marco Fasani**

**Responsabilità: Valutare la conformità alle normative e politiche interne, revisionare i piani di contingenza.**

## **Database Administrator:**

**Nome: Sara Spaccialbelli**

**Responsabilità: Assicurare che i controlli di sicurezza del database siano implementati correttamente e gestire l'integrità dei dati.**

## **Network Security Engineer:**

**Nome: Angelo Di Mauro**

**Responsabilità: Verificare la sicurezza della rete, inclusa la protezione delle trasmissioni dei dati e la gestione delle configurazioni di rete.**

# Report di Assessment:

Controllo	Stato	Risultanze	Raccomandazioni	Commenti
CP-2	Conforme	Piano di contingenza aggiornato e testato	Continuare con test regolari	Verificare efficacia annuale
RA-5	Non conforme	Scansioni di vulnerabilità non regolari	Implementare scansioni mensili	Aggiornare programma di scansioni
AC-3	Conforme	Politiche di accesso ben implementate	Nessuna	Politiche aggiornate di recente
SA-11	Conforme	Test di sicurezza documentati	Continuare con test regolari	Documentare tutti i test
SC-8	Parzialmente conforme	Protezione dati con alcune lacune	Implementare crittografia end-to-end	Aggiungere protezioni extra

- 1** Definire i test
- 2** Avviare audit
- 3** Audit attivi
- 4** Audit passati

Quadro di controllo:			Famiglia di controllo:			Nome controllo:																					
<input type="button" value="TUTTI (3)"/>			<input type="button" value="Nessun"/>			<input type="text"/>																					
<p><b>Controllo nome lungo:</b> Scansioni delle vulnerabilità</p> <p><b>Proprietario del controllo:</b></p> <p><b>Descrizione:</b></p> <p style="text-align: right;"><b>Aggiungi test</b></p>																											
<table border="1"> <thead> <tr> <th>ID</th> <th>Nome del test</th> <th>Tester</th> <th>Altre parti interessate</th> <th>Tag</th> <th>Frequenza di prova</th> <th>Ultima data di test</th> <th>Prossima prova data</th> <th>Tempo approssimativo</th> </tr> </thead> <tbody> <tr> <td>2</td> <td>Nessus</td> <td>Angelo Di Mauro</td> <td>Angelo Di Mauro</td> <td></td> <td>60 giorni</td> <td>04/21/2024</td> <td>06/20/2024</td> <td>150 minuti</td> <td> </td> </tr> </tbody> </table>									ID	Nome del test	Tester	Altre parti interessate	Tag	Frequenza di prova	Ultima data di test	Prossima prova data	Tempo approssimativo	2	Nessus	Angelo Di Mauro	Angelo Di Mauro		60 giorni	04/21/2024	06/20/2024	150 minuti	
ID	Nome del test	Tester	Altre parti interessate	Tag	Frequenza di prova	Ultima data di test	Prossima prova data	Tempo approssimativo																			
2	Nessus	Angelo Di Mauro	Angelo Di Mauro		60 giorni	04/21/2024	06/20/2024	150 minuti																			
<p><b>Controllo nome lungo:</b> Control Assessments Assess the controls in accordance with the assessment procedures described in assessment plans.</p> <p><b>Proprietario del controllo:</b></p> <p><b>Descrizione:</b></p> <p style="text-align: right;"><b>Aggiungi test</b></p>																											
<table border="1"> <thead> <tr> <th>ID</th> <th>Nome del test</th> <th>Tester</th> <th>Altre parti interessate</th> <th>Tag</th> <th>Frequenza di prova</th> <th>Ultima data di test</th> <th>Prossima prova data</th> <th>Tempo approssimativo</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>Verifica dei controlli</td> <td>Angelo Di Mauro</td> <td></td> <td></td> <td>30 giorni</td> <td>04/13/2024</td> <td>05/22/2024</td> <td>30 minuti</td> <td> </td> </tr> </tbody> </table>									ID	Nome del test	Tester	Altre parti interessate	Tag	Frequenza di prova	Ultima data di test	Prossima prova data	Tempo approssimativo	3	Verifica dei controlli	Angelo Di Mauro			30 giorni	04/13/2024	05/22/2024	30 minuti	
ID	Nome del test	Tester	Altre parti interessate	Tag	Frequenza di prova	Ultima data di test	Prossima prova data	Tempo approssimativo																			
3	Verifica dei controlli	Angelo Di Mauro			30 giorni	04/13/2024	05/22/2024	30 minuti																			
<p><b>Controllo nome lungo:</b> Test di sicurezza</p> <p><b>Proprietario del controllo:</b></p> <p><b>Descrizione:</b></p> <p style="text-align: right;"><b>Aggiungi test</b></p>																											
<table border="1"> <thead> <tr> <th>ID</th> <th>Nome del test</th> <th>Tester</th> <th>Altre parti interessate</th> <th>Tag</th> <th>Frequenza di prova</th> <th>Ultima data di test</th> <th>Prossima prova data</th> <th>Tempo approssimativo</th> </tr> </thead> <tbody> <tr> <td>5</td> <td>PenTest</td> <td>Angelo Di Mauro</td> <td></td> <td></td> <td>60 giorni</td> <td>03/22/2024</td> <td>05/22/2024</td> <td>360 minuti</td> <td> </td> </tr> </tbody> </table>									ID	Nome del test	Tester	Altre parti interessate	Tag	Frequenza di prova	Ultima data di test	Prossima prova data	Tempo approssimativo	5	PenTest	Angelo Di Mauro			60 giorni	03/22/2024	05/22/2024	360 minuti	
ID	Nome del test	Tester	Altre parti interessate	Tag	Frequenza di prova	Ultima data di test	Prossima prova data	Tempo approssimativo																			
5	PenTest	Angelo Di Mauro			60 giorni	03/22/2024	05/22/2024	360 minuti																			
<p><b>Controllo nome lungo:</b> Protezione dei dati in trasmissione</p> <p><b>Proprietario del controllo:</b></p> <p><b>Descrizione:</b></p> <p style="text-align: right;"><b>Aggiungi test</b></p>																											
<table border="1"> <thead> <tr> <th>ID</th> <th>Nome del test</th> <th>Tester</th> <th>Altre parti interessate</th> <th>Tag</th> <th>Frequenza di prova</th> <th>Ultima data di test</th> <th>Prossima prova data</th> <th>Tempo approssimativo</th> </tr> </thead> <tbody> <tr> <td>6</td> <td>Controllo traffico di rete</td> <td>Angelo Di Mauro</td> <td></td> <td></td> <td>1 Giorno</td> <td>05/21/2024</td> <td>05/22/2024</td> <td>1440 minuti</td> <td> </td> </tr> </tbody> </table>									ID	Nome del test	Tester	Altre parti interessate	Tag	Frequenza di prova	Ultima data di test	Prossima prova data	Tempo approssimativo	6	Controllo traffico di rete	Angelo Di Mauro			1 Giorno	05/21/2024	05/22/2024	1440 minuti	
ID	Nome del test	Tester	Altre parti interessate	Tag	Frequenza di prova	Ultima data di test	Prossima prova data	Tempo approssimativo																			
6	Controllo traffico di rete	Angelo Di Mauro			1 Giorno	05/21/2024	05/22/2024	1440 minuti																			

# Inserimento in SimpleRisk

- Navigare alla sezione "Compliance" di SimpleRisk.
  - Aggiungere un nuovo assessment per ciascun controllo specifico.
- inserendo:**
- obiettivi
  - tag
  - squadra
  - frequenza di prova
  - ultima data test
  - prossima prova data
  - passi di prova
  - tempo approssimativo
  - risultati attesi
  - le risultanze, includendo conformità, non conformità, raccomandazioni e commenti.

# Progetto S4/L5

## **Gestione del rischio informatico per un caso aziendale specifico - Assessment, Authorize e Monitor**

**Alex Fiorillo**

**Andrea Dura**

**Angelo Di Mauro**

**Marco D'antoni**

**Marco Fasani**

**Sara Spaccialbelli**



**Task****Descrizione**

**TASK A-5**  
**Remediation**  
**Actions Conduct**  
**initial remediation**  
**actions on the**  
**controls and**  
**reassess**  
**remediated**  
**controls.**

**Obiettivo:** Attuare azioni correttive per risolvere le problematiche emerse durante l'assessment.

**Attività da Svolgere:**

- **Analisi delle Non Conformità:**
- **Rivedere i risultati dell'assessment per identificare i controlli non conformi.**
- **Prioritizzare le non conformità basandosi sulla criticità e sull'impatto.**
- **Pianificazione delle Azioni di Rimedio:**
- **Definire le azioni correttive specifiche per ogni non conformità.**
- **Stabilire un calendario per l'implementazione delle azioni correttive.**
- **Implementazione delle Azioni:**
- **Assegnare responsabilità per l'implementazione delle azioni correttive ai membri del team.**
- **Eseguire le azioni correttive secondo il piano stabilito.**

**Monitoraggio e Verifica:**

- **Monitorare l'avanzamento delle azioni correttive.**
- **Verificare l'efficacia delle azioni correttive una volta implementate.**

**Azioni Correttive per i Controlli Non Conformi:**

- **RA-5 (Scansioni di Vulnerabilità):**
- **Azione Correttiva:** Implementare scansioni di vulnerabilità mensili.
- **Responsabile:** Security Analyst
- **Tempistica:** Entro il 30 giugno 2024
- **SC-8 (Protezione dei Dati in Trasmissione):**
- **Azione Correttiva:** Implementare crittografia end-to-end.
- **Responsabile:** Network Security Engineer
- **Tempistica:** Entro il 15 luglio 2024

**Output del Task A-5:**

- **Registro delle Azioni Correttive:** Dettagli delle azioni intraprese, inclusi responsabili e tempistiche.
- **Aggiornamenti su SimpleRisk:** Inserire le azioni correttive nel campo commento dei test rilevanti e aggiornare lo stato dei controlli e rischi.

**Task****Descrizione**

**TASK A-6 Plan of Action and Milestones**  
Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.

**Obiettivo:** Decidere se implementare immediatamente le azioni correttive o posticiparle, motivando la decisione.

**Attività da Svolgere:**

**Valutazione della Fattibilità:**

- Valutare le risorse e i tempi necessari per implementare le azioni correttive.
- Considerare l'impatto sull'operatività aziendale.

**Decisione sull'Implementazione:**

- **Implementazione Immediata:** Se le risorse sono disponibili e l'azione è critica.
- **Posticipazione:** Se le risorse non sono disponibili o se l'azione non è critica.

**Pianificazione delle Azioni Future:**

- Definire un calendario per le azioni correttive posticipate.
- Documentare le motivazioni per il posticipo.

**Azioni Pianificate e Motivazioni:**

- RA-5 (Scansioni di Vulnerabilità):
- **Decisione:** Implementare scansioni di vulnerabilità mensili immediatamente.
- **Motivazione:** Criticità elevata, impatto diretto sulla sicurezza.
- SC-8 (Protezione dei Dati in Trasmissione):
- **Decisione:** Posticipare l'implementazione della crittografia end-to-end.
- **Motivazione:** Risorse limitate, priorità data a interventi più critici.
- **Pianificazione:** Entro il 30 settembre 2024

**Output del Task A-6:**

- **Registro delle Decisioni:** Documentazione delle decisioni prese, con motivazioni e tempistiche.
- **Aggiornamenti su SimpleRisk:** Inserire le decisioni e pianificazioni nel campo commento dei test rilevanti.

**Task****Descrizione**

**TASK R-1**  
**Authorization**  
**Package Assemble**  
**the authorization**  
**package and**  
**submit the**  
**package to the**  
**authorizing official**  
**for an**  
**authorization**  
**decision.**

**Obiettivo:** Presentare alla direzione un report dettagliato sui rischi rilevati nei due sistemi (ERP-HQ e ERP-BR) e i costi associati ai trattamenti, affinché la direzione possa approvare o rifiutare le proposte di mitigazione.

**Componenti del Report:**

**1. Sintesi dell'Assessment:**

- Breve descrizione dell'analisi dei rischi effettuata.
- Panoramica dei controlli esaminati e delle non conformità rilevate.

**2. Lista dei Rischi Identificati:**

- Descrizione dettagliata di ogni rischio.
- Livello di criticità (alto, medio, basso).
- Probabilità di occorrenza e impatto.

**3. Proposte di Trattamento dei Rischi:**

- Dettaglio delle azioni correttive suggerite per ogni rischio.
- Costi stimati per l'implementazione delle azioni correttive.
- Percentuale di mitigazione prevista per ogni trattamento.

**4. Budget Totale:**

- Sommario dei costi totali per tutte le azioni correttive proposte.

Task	Descrizione
<p><b>TASK R-3 Risk Response Identify and implement a preferred course of action in response to the risk determined.</b></p>	<p><b>Attività da Svolgere:</b></p> <ol style="list-style-type: none"> <li><b>1. Riunione con la Direzione:</b> <ul style="list-style-type: none"> <li>○ Presentare il report alla direzione simulata.</li> <li>○ Fornire spiegazioni dettagliate per ogni rischio e trattamento proposto.</li> <li>○ Rispondere a domande e fornire ulteriori chiarimenti.</li> </ul> </li> <li><b>2. Decisioni della Direzione:</b> <ul style="list-style-type: none"> <li>○ La direzione approverà o respingerà ogni proposta di trattamento.</li> <li>○ Ogni decisione sarà motivata (ad esempio, basata su budget, impatto, priorità aziendali).</li> </ul> </li> <li><b>3. Documentazione delle Decisioni:</b> <ul style="list-style-type: none"> <li>○ Registrare le decisioni della direzione e le relative motivazioni.</li> <li>○ Esempio di report della direzione: <ul style="list-style-type: none"> <li>■ RA-5: Approvato. La scansione mensile delle vulnerabilità è critica per la sicurezza del sistema. Costo accettabile.</li> <li>■ SC-8: Respinto. Costi elevati, considerare alternative meno costose per la crittografia.</li> <li>■ AC-3: Approvato. Importante mantenere politiche di accesso aggiornate.</li> <li>■ CP-2: Approvato. Aggiornamento del piano di contingenza essenziale per la continuità operativa.</li> <li>■ SA-11: Respinto. Priorità bassa, possibile revisione in futuro.</li> </ul> </li> </ul> </li> <li><b>4. Implementazione delle Azioni Approvate:</b> <ul style="list-style-type: none"> <li>○ Procedere con l'implementazione delle azioni correttive approvate dalla direzione.</li> <li>○ Pianificare le azioni correttive future per quelle respinte, considerando soluzioni alternative.</li> </ul> </li> </ol>

# Tabella dei Rischi e Trattamenti

Rischio	documentazione	Criticità	Azione Correttiva	Costo	% di mitigazione	Stato
RA-5	Scansioni di vulnerabilità non regolari, rischio di esposizione a minacce non rilevate.	Alta	Implementare scansioni mensili	3.000	90%	In attesa
SC-8	Protezione dati in trasmissione insufficiente, rischio di intercettazione.	Alta	Implementare crittografia end-to-end	5.000	95%	In attesa
AC-3	Politiche di controllo accessi necessitano revisione periodica, rischio di accessi non autorizzati.	Media	Revisione trimestrale delle politiche	1.500	80%	In attesa
CP-2	Piano di contingenza non aggiornato, rischio di inefficacia in caso di disastro.	Media	Aggiornamento piano di contingenza	2.500	85%	In attesa
SA-11	Test di sicurezza non documentati, rischio di falle non rilevate nei sistemi di sicurezza.	Bassa	Documentazione e test regolari	1.000	75%	In attesa

EXAMPLE

Governance La Gestione Del Rischio Conformità Asset Management Valutazioni Reporting Configurare

Ricerca Angelo Di Mauro

Risk ID: ID: 1005 Task P-1

Rischio intrinseco: 6 | Rischio residuo: 3.6 | Stato: Mitigation Planned | Subject: TASK P-14 / Interruzione del servizio

Dettagli | Di mitigazione | Recensione

Mappatura dei rischi: Business interruption  
Mappatura delle minacce: Hacking & Other Cybersecurity Crimes  
Data Di Presentazione: 05/20/2024  
CATEGORIA: Technical Vulnerability Management  
Sito/Posizione: on-premises, Cloud  
Esterno ID di Riferimento:  
Regolamento Di Controllo: MIST 800-53  
Numero Di Controllo: CP-2  
Asset: Application, DB, ERP-BR, ERP-HQ  
Tecnologia: Backups, Datacenter, Network, Remote Access, Web  
Squadra: Data Center & Storage, Database, IT Systems Management, Network, Web Systems  
Altri parti interessate:  
Proprietario: Angelo Di Mauro  
Manager del proprietario: Angelo Di Mauro  
Tag:  
Nessun tag assegnato ancora.

**Commenti**

05/23/2024 2:58 AM CDT by Angelo Di Mauro

Azione Correttiva: Implementare scansioni di vulnerabilità iniziali.  
Responsabile: Security Analyst  
Tempistica: Entro il 30 giugno 2024  
SC-8 (Protezione dei Dati in Transfert):  
Azione Correttiva: Implementare critografia end-to-end.  
Responsabile: Network Security Engineer  
Tempistica: Entro il 15 luglio 2024

Audit Trail

Vedi rischio seguendo dettagli  
Visualizza il Punteggio di rischio nel tempo

Rischio intrinseco: 6 | Rischio residuo: 3.6 | Stato: Mitigation Planned | Subject: TASK P-14 / Interruzione del servizio

Dettagli | Di mitigazione | Recensione

Data di presentazione di: 05/21/2024  
mitigazione:  
Data di mitigazione prevista: 05/21/2024  
Strategia Di Pianificazione: Mitigate  
Sforzo Di Mitigazione: Considerabile  
Riduzione Dei Costi: \$100,000 to \$200,000  
Di Mitigazione Dell'Proprietario: Angelo Di Mauro  
Di Mitigazione Del Team: Data Center & Storage, Database, IT Systems Management, Network, Web Systems  
Per cento di mitigazione: 40%  
Mitigation accepted by Angelo Di Mauro on 05/23/2024 at 03:36  
Rifiuta attenuazione

Soluzione Comitita: Messi server di ridondanza, Gruppo PSU  
Requisiti Di Sicurezza: requisiti di sicurezza per un gruppo di continuità (PSU, Power Supply Unit) sono fondamentali per garantire la sicurezza elettrica, prevenire danni ai dispositivi collegati e proteggere gli utenti. Ecco un riassunto dei principali requisiti di sicurezza per un PSU: Certificazioni di Sicurezza CE (Conformité Européenne): Indica che il PSU è conforme agli standard di sicurezza dell'Unione Europea. UL (Underwriters Laboratories): Certificazione nordamericana che garantisce che il PSU soddisfa specifici standard di sicurezza. TÜV (Technischer Überwachungsverein): Certificazione tedesca che attesta la conformità agli standard di sicurezza europei e internazionali. FCC (Federal Communications Commission): Certificazione che assicura che il PSU non interferisce con altri dispositivi elettronici. Protezione contro sovratensioni e sovraccarichi: il PSU deve essere dotato di sistemi di protezione che preservino danni da sovratensioni, sovraccarichi, cortocircuiti e sbalzi di tensione.

Raccomandazioni Per La Sicurezza:  
La Documentazione Di Supporto: Nessuno

# La Mitigation

# Report della Direzione

Rischio	Stato	motivazione
RA-5	Approvato	Critico per la sicurezza, costo accettabile.
SC-8	Respinto	Costi elevati, considerare alternative meno costose.
AC-3	Approvato	Importante mantenere politiche di accesso aggiornate.
CP-2	Approvato	Essenziale per la continuità operativa.
SA-11	Respinto	Priorità bassa, possibile revisione in futuro.

**Sulla base del report della direzione,  
il team procederà con l'implementazione delle azioni correttive,  
approvate  
e pianificherà le azioni future per i trattamenti respinti.**

A red rectangular stamp with the word "EXAMPLE" written diagonally across it, centered within a white circle.

# Presentazione Finale del Progetto e Strategie di Monitoraggio

**Obiettivo:** Concludere il progetto con una presentazione dettagliata delle attività svolte, dei risultati ottenuti e delle strategie di monitoraggio per assicurare la continua gestione dei rischi e la sicurezza del sistema.

## Sommario della Presentazione

### Introduzione

L'obiettivo del progetto è stato quello di analizzare i rischi legati ai sistemi ERP-HQ e ERP-BR, sviluppare strategie di mitigazione e implementare un monitoraggio continuo. Durante la settimana sono state completate diverse attività chiave:

### Riepilogo delle Task

Abbiamo selezionato un gruppo di assessment (Task P-2), sviluppato un piano di assessment (Task P-8), identificato i rischi (Task P-9) e valutato i rischi (Task P-10). Le informazioni per l'assessment sono state raccolte (Task P-11), e le attività di assessment sono state realizzate (Task P-12). I risultati dell'assessment sono stati documentati (Task P-13) e i controlli sono stati revisionati e approvati (Task P-16).

### Rischi Identificati e Valutazione

Durante l'assessment, sono stati identificati e valutati diversi rischi. Ogni rischio è stato descritto dettagliatamente, con indicazione del livello di criticità, probabilità e impatto. Abbiamo anche stimato i costi per le azioni correttive proposte.

### Decisioni della Direzione (Task R-1 e R-3)

Abbiamo presentato alla direzione un report sui rischi e i costi di trattamento. La direzione ha approvato alcune azioni correttive e ne ha respinte altre, fornendo motivazioni basate su budget, impatto e priorità aziendali. Le azioni correttive approvate sono state pianificate per l'implementazione.

# conclusioni

## Strategie di Monitoraggio

**Il monitoraggio continuo è essenziale per garantire l'efficacia dei controlli di sicurezza e identificare nuovi rischi. Utilizziamo SimpleRisk per registrare e monitorare i rischi e i controlli. Le scansioni di vulnerabilità vengono effettuate mensilmente, gli audit interni sono trimestrali, le politiche di sicurezza vengono riviste semestralmente e il piano di contingenza viene aggiornato annualmente. Le responsabilità di monitoraggio sono distribuite tra il Security Analyst, il Compliance Officer, l'IT Specialist, il Database Administrator e il Network Security Engineer.**

## Conclusione

**Il progetto ha portato all'implementazione di azioni correttive importanti e ha stabilito un piano di monitoraggio continuo per garantire la sicurezza dei sistemi ERP-HQ e ERP-BR. I prossimi passi includono l'implementazione delle azioni future per i rischi respinti e miglioramenti continui. La documentazione finale comprende un report completo dell'assessment e aggiornamenti su SimpleRisk.**

**Questa presentazione finale fornisce un quadro completo del lavoro svolto e delle strategie future per mantenere la sicurezza e la conformità dei sistemi aziendali.**



# Progetto S4

**Questa presentazione  
è stata offerta da:**

**Alex Fiorillo**

**Andrea Dura**

**Angelo Di Mauro**

**Marco D'antoni**

**Marco Fasani**

**Sara Spaccialbelli**

