

S4 - L1

Gestione del rischio informatico per un caso aziendale specifico - Prepare

17 maggio 2024

Team

- Davide Di Turo
- Lisa Bonato
- Manuel Di Gangi
- Maria Flavia Minotti
- Oliviero Camarota

INDICE

Traccia - Giorno 1 - Prepare	3
1.1 - Progetto guidato settimanale.....	3
1.2 - Caso aziendale.....	3
1.3 - Specifiche middleware.....	4
1.4 - Scenario attuale.....	5
1.5 - Creazione dell'architettura di partenza (opzione 1).....	6
1.6 - Creazione dell'architettura alternativa (opzione 2).....	7
2. Infrastruttura di rete proposta	8
3. Prepare – Organization Level	9
4. Prepare – System Level	10
5. Inserimento Asset in SimpleRisk	12
6. Architettura di rete	15
6.1 - Analisi dell'architettura.....	15
6.2 - Note Finali.....	16
6.3 - Politiche di Accesso.....	17
Traccia - Giorno 2 - Prepare e Categorize	17
1. Categorize	18

Traccia - Giorno 1 - Prepare

1.1 - Progetto guidato settimanale

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*:

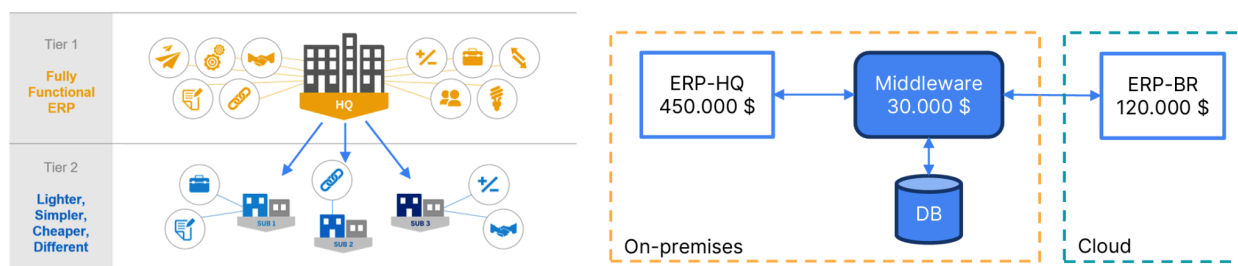
- Prepare
- Categorize
- Select
- Implement
- Assess
- Authorize
- Monitor

Si consiglia la suddivisione in gruppi a partire già da oggi. * Sono stati selezionati un sottoinsieme di task per far rientrare l'intero processo in una settimana.

1.2 - 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.



1.3 - 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

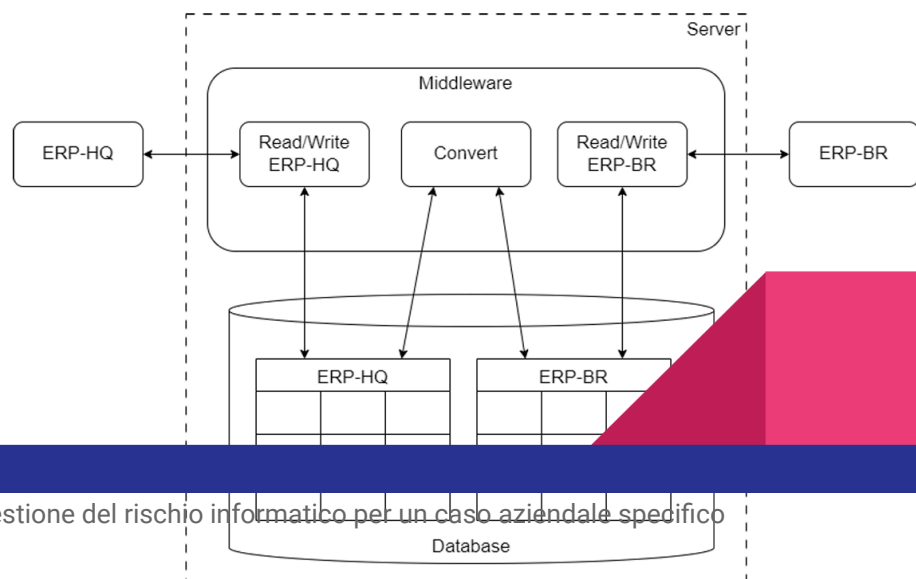
indipendenti e hanno un proprio database). I due moduli Read/Write ERP-HQ e ERP-BR si occupano di leggere/scrivere i dati di transito nel db interno tra ERP-HQ/Middleware e ERP-BR/Middleware. Middleware e database di supporto, risiedono sullo stesso server on-premises, ma differente dall'ERP-HQ. Il Middleware 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.

1.4 - Scenario attuale

Da qualche giorno, l'azienda che ha 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 perché permette di sincronizzare i due ERP, ad esempio, magazzino, impianti di produzione, utenti, fatturazione, ecc. Adesso, l'organizzazione deve valutare se:

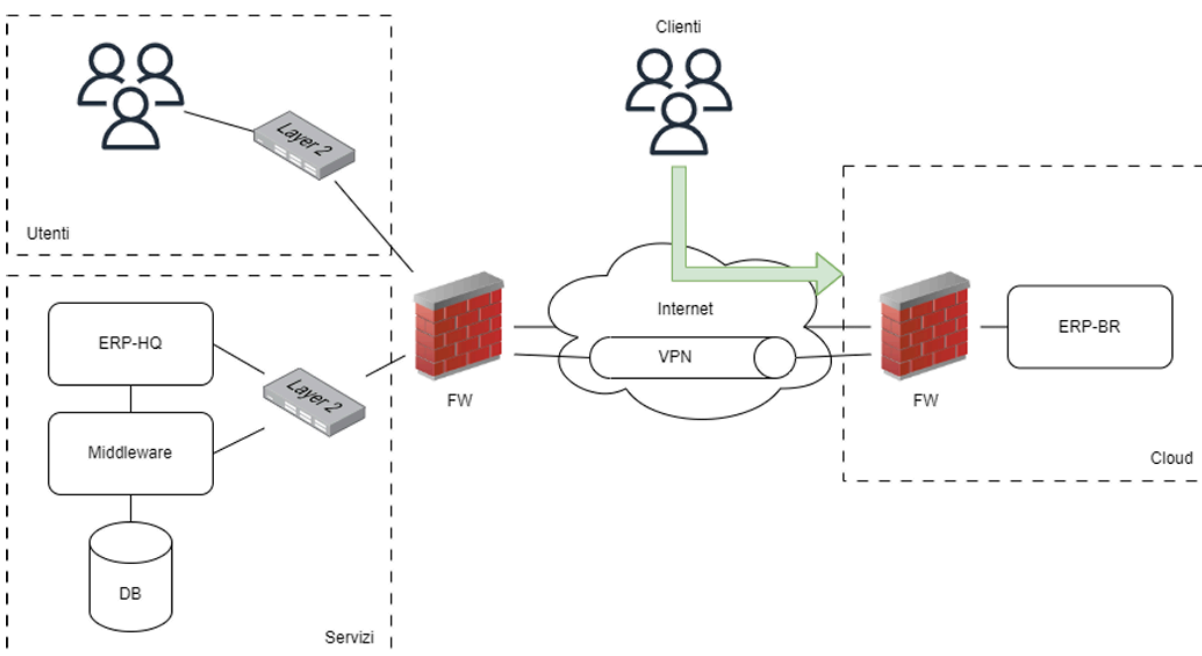
1. continuare a mantenere questo middleware on-premises, di cui non conosce molto, trovando un nuovo fornitore in grado di fare un'analisi approfondita (compreso reverse engineering) per poterne continuare lo sviluppo, oppure,
2. sostituire il middleware con una soluzione SaaS/iPaaS di data integration/automation, 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.



1.5 - 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.



1.6 - Creazione dell'architettura alternativa (opzione 2)

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

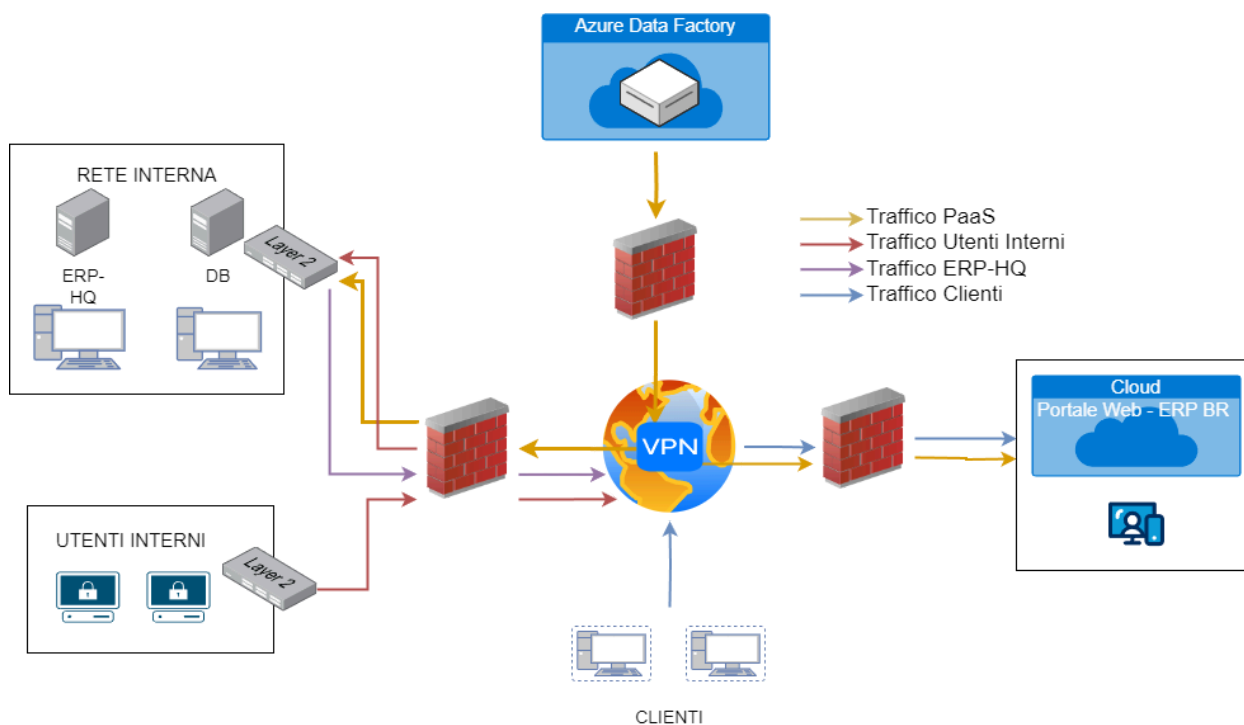
2. sostituire il middleware con una soluzione SaaS/iPaaS di data integration/automation, possibilmente low-code/nocode per evitare l'affidamento ad un'altra software house e gestire il solo mapping delle strutture dati con le risorse interne (dipendenti).

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 open source, 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/>
- <https://marjory.io/>

2. Infrastruttura di rete proposta



Come si può dedurre dallo schema di rete ideato, si è deciso di analizzare l'opzione 2 prevedendo che il middleware sia sostituito da una soluzione PaaS basata su cloud.

Al centro si è inserita la connessione internet con la VPN che consente il collegamento tra le varie della rete aziendale. In alto, la soluzione PaaS protetta da Firewall in modo da controllare il flusso verso il Provider del servizio.

A destra si rappresenta il software ERP-BR, anch'esso in cloud, con relativo portale web a cui hanno accesso i clienti dell'organizzazione.

A sinistra vediamo l'intranet aziendale con la VLAN dei dipendenti e la VLAN dei servizi nella quale permane il server che ospita l'ERP-HQ ed il DB.

3. 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 task a Simple Risk. Per differenziare le entità relative a opzione 1 e 2, utilizzate tag.

Task	Descrizione	Simple Risk
TASK P-2 Risk Management Strategy Establish a risk management strategy for the organization that includes a determination of risk tolerance.	<p>Stabilire una strategia di gestione del rischio che guidi e informi le decisioni basate sul rischio, incluso come il rischio di sicurezza e privacy è inquadrato, valutato, affrontato e monitorato.</p> <p>L'azienda ha stabilito un livello di tolleranza del rischio medio-bassa, con l'obiettivo di minimizzare i rischi di sicurezza delle informazioni e garantire la business continuity. La strategia deve considerare la gestione del rischio della catena di approvvigionamento (SCRM).</p> <p>Inoltre, deve includere le decisioni e le considerazioni a livello strategico su come i leader senior e i dirigenti devono gestire i rischi di sicurezza e privacy (inclusi i rischi della catena di approvvigionamento)</p>	<p>Configurare i valori di rischio, matrici, formula, ecc.</p> <p>TAG: Opzione 1 e 2.</p>
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.	<p>L'organizzazione prevede l'uso del NIST SP 800-53 per selezionare e personalizzare i controlli di sicurezza rilevanti e del NIST CSF per sviluppare profili di cybersecurity adattati alle esigenze dell'organizzazione.</p> <p>Le attività principali includono: Identificare e adattare i controlli di sicurezza del NIST SP 800-53 in base alle esigenze specifiche dell'organizzazione. Sviluppare profili del NIST CSF per definire i livelli di implementazione dei controlli in base alla valutazione del rischio e ai requisiti operativi.</p>	<p>Definire i framework che si intendono utilizzare (tra quelli visti nel corso), Governance/1/Framework orks.</p>

	<p>Documentare dettagliatamente i baseline di controllo e i profili di cybersecurity, rendendoli accessibili agli stakeholder rilevanti. .</p> <p>Stabilire un processo di revisione periodica per aggiornare e migliorare continuamente i controlli e i profili in risposta ai cambiamenti nelle minacce, nei requisiti normativi e nelle operazioni aziendali.</p>	
--	--	--

4. Prepare – System Level

Task	Descrizione	Simple Risk
TASK P-8 Mission or Business Focus Identify the missions, business functions, and mission/business processes that the system is intended to support.	<p>L'opzione 2 selezionata è progettata per supportare la funzione prioritaria di integrazione e sincronizzazione dei dati dei due ERP, in modo da ottenere una gestione integrata di ordini, vendite, inventario e fatturazione.</p> <p>Per comprendere efficacemente questa funzione aziendale è essenziale coinvolgere gli stakeholder (Identificazione al task P-9) in modo da guidare anche le decisioni sul rischio, comprese quelle relative all'architettura aziendale, e di sicurezza e privacy correlate.</p>	TAG: 2
TASK P-9 System Stakeholders Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.	<p>Gli stakeholder coinvolti sono:</p> <ul style="list-style-type: none"> - Il team di sviluppo responsabile della configurazione del servizio iPaaS - Azure data factory - Il fornitore del servizio IPaaS - Azure data factory - Il team tecnico responsabile della gestione / manutenzione del sistema - Gli utenti interni - Il team di Security - I clienti 	TAG: 2
TASK P-10 Asset Identification Identify assets that require protection.	<ul style="list-style-type: none"> - PaaS - Azure Data Factory - Portale web 	<p>Asset management*</p> <p>TAG: 2</p>

	<ul style="list-style-type: none"> - Configurazione e mappatura dei dati sul nuovo servizio PaaS - Infrastruttura di rete aziendale (Compresi Firewall perimetrali) - Dati utenti - ERP -HQ - ERP -BR - Personale - Immagine aziendale 	
TASK P-11 Authorization Boundary Determine the authorization boundary of the system.	Responsabilità dell'utente: Sicurezza delle applicazioni. Gestione dei dati e protezione delle informazioni sensibili. Configurazione della sicurezza delle applicazioni. Controllo degli accessi e gestione delle identità.	Tag: 2
TASK P-12 Information Types Identify the types of information to be processed, stored, and transmitted by the system.	<p>Le informazioni maneggiate dall'organizzazione riguardano:</p> <ul style="list-style-type: none"> - Dati di inventario (prodotti, quantità, prezzi) - Dati di ordine (dettagli dell'ordine, informazioni di spedizione, informazioni di pagamento) - Dati di fatturazione (fatture, pagamenti, sconti) - Dati personali dei clienti (nome, indirizzo, informazioni di contatto). 	<p>Anche le informazioni sono asset.</p> <p>TAG: 2</p>
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.	<p>Creazione: I dati vengono creati in uno dei due ERP</p> <p>Elaborazione: I dati vengono elaborati e trasformati dal servizio PaaS per essere sincronizzati</p> <p>Memorizzazione: I dati vengono memorizzati nel servizio PaaS durante il processo di sincronizzazione</p> <p>Trasmissione: I dati vengono trasmessi tra ERP-HQ, PaaS e ERP-BR attraverso la VPN dedicata</p> <p>Archiviazione: I dati vengono archiviati nei database del PaaS</p> <p>Eliminazione: I dati vengono eliminati dai database solo su richiesta specifica</p>	TAG: 2
TASK P-14 Risk Assessment—System Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.	Valutazione del rischio in caso di attacco DDos e Data breach	Risk Management/1
TASK P-16 Enterprise Architecture Determine the placement of the system within the enterprise architecture.	Architettura riportata al punto 2. <i>Architettura di rete proposta</i> , analizzata al punto 6. <i>Architettura di rete</i>	TAG: 2

* Anche se i sistemi da gestire in SimpleRisk sono due (opzione 1 e 2), questi condividono molte 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. Opzione 1, Opzione 2, Entrambi).

5. Inserimento Asset in SimpleRisk

The screenshots show the 'Configure' page in SimpleRisk, specifically the 'Add and Remove Values' section under 'Site/Location'.

Top Screenshot:

- Select:** Site/Location
- Site/Location:**
 - Add new item named: On-premise [Add]
 - Change -- [v] to [] [Update]
 - Delete item named: -- [v] [Delete]

Bottom Screenshot:

- Select:** Site/Location
- Site/Location:**
 - Add new item named: Cloud [Add]
 - Change -- [v] to [] [Update]
 - Delete item named: -- [v] [Delete]

Per lo svolgimento del processo di gestione del rischio si utilizzerà SimpleRisk, una piattaforma integrata per la gestione della governance, del rischio e della conformità (GRC).

Il primo passo del processo è l'inserimento degli asset sulla base dei quali si procederà ad identificare e analizzare il rischio. Su "**Configure**", "**Add and Remove Values**" selezioniamo **Site/Location** per inserire (**Add**) il luogo, fisico o immateriale, in cui si trovano gli asset: On-premise e Cloud.

The screenshot shows the 'Add a New Asset' form in the 'Asset Management' section. The sidebar on the left has three steps: 1. Automated Discovery, 2. Manage Assets (highlighted), and 3. Manage Asset Groups. The form fields are as follows:

- Asset Name:** ADF - Azure Data Factory
- IP Address:** (empty)
- Asset Valuation:** \$0 to \$100,000
- Site/Location:** Cloud
- Team:** Collaboration
- Associated Risks:** None selected
- Asset Details:** A rich text editor containing the text: "Soluzione iPaaS/SaaS che mette a disposizione servizio Mapping Data Flows per pianificare e gestire i flussi di lavoro di integrazione e trasformazione dei dati senza necessità di scrivere codice (no-code). Quindi, l'organizzazione ha il controllo completo sul mapping delle strutture dati e sulla configurazione delle attività di integrazione e i suoi dipendenti sono in grado di definire e gestire autonomamente il mapping dei dati senza fare affidamento su terze parti o sviluppatori esterni."
- Mapped Controls:** A table with columns: Current Maturity, Control, and Actions.
- Tags:** Opzione 2

At the bottom right, there is a red text warning: "The maximum length of a tag is 255 characters."





Si procede poi all'inserimento degli Asset principali spostandosi nel tab "**Asset Management**" e "**Manage Assets**".

Per ciascuno degli Asset, come si può vedere nell'esempio della figura sopra relativo all'**inserimento dell' ADF**, si sono inseriti, in ordine, il valore, il luogo, il team responsabile e i dettagli, nel quale si rinviene descrizione esplicitativa degli stessi.

In “tag” si è inserito per tutti gli asset “opzione 2”, visto che è quella in analisi.

Per finalizzare l'inserimento, ancora una volta si seleziona “Add”.

A questo punto sarà possibile visionare l’**elenco degli asset inseriti - ADF, Configurazione e mappatura dati sul PaaS, ERP-BR, ERP-HQ, Immagine aziendale, Network, Personale, Portale Web** - nella parte inferiore della schermata dell’ “Asset Management”.

Verified Assets							
Delete All							
Actions	Asset Name	IP Address	Asset Valuation	Site/Location	Team	Asset Details	Tags
	Asset Name	IP Address	Asset Valuation	Site/Location	Team	Asset Details	Tags
 	ADF - Azure Data Factory		\$0 to \$100,000	Cloud	Collaboration	Soluzione iPaaS/SaaS che mette a disposizione servizio Mapping Data Flows per pianificare e gestire i flussi di lavoro di integrazione e trasformazione dei dati senza necessità di scrivere codice (no-code). Quindi, l'organizzazione ha il controllo completo sul mapping delle strutture dati e sulla configurazione delle attività di integrazione e i suoi dipendenti sono in grado di definire e gestire autonomamente il mapping dei dati senza fare affidamento su terze parti o sviluppatori esterni.	Opzione 2
 	Configurazione e mappatura dei dati sul PaaS		\$0 to \$100,000	Cloud	Data Center & Storage, Database, Information Security		Opzione 2
 	Dati degli utenti		\$400,001 to \$500,000	All Sites	Data Center & Storage, Database, Information Security	L'azienda gestisce informazioni sensibili degli utenti tra cui dati finanziari. Queste informazioni sono processate e archiviate sia su ERP-HQ che ERP-BR e sulla soluzione PaaS.	Opzione 2
 	ERP-BR		\$100,001 to \$200,000	Cloud	IT Systems Management	TIER 2: Gestionale delle filiali. Separato rispetto al ERP-HQ, è più snello, flessibile e permette di avere una certa autonomia nella gestione delle operazioni, tenendo conto dei processi localizzati. Costo: 120.000. Di solito un Tier 2 non è in grado di vedere altri Tier 2.	Opzione 1 Opzione 2
 	ERP-HQ		\$400,001 to \$500,000	On-premise	IT Systems Management	TIER 1: Gestionale della sede principale dell'organizzazione: centralizzato, robusto, in grado di gestire operazioni e requisiti generali dell'organizzazione. Costo: 450.000.	Opzione 1 Opzione 2
 	Immagine aziendale		\$900,001 to \$1,000,000			Per immagine aziendale si fa riferimento ad una categoria di asset intangibili - fiducia nell'organizzazione di clienti e stakeholders e, a cascata, la reputazione e il brand della stessa - che riveste un'importanza fondamentale poiché, se intaccata, genera costi ingenti per eventuali richieste di risarcimento, sanzioni, perdite di investimenti e profitti.	Opzione 2

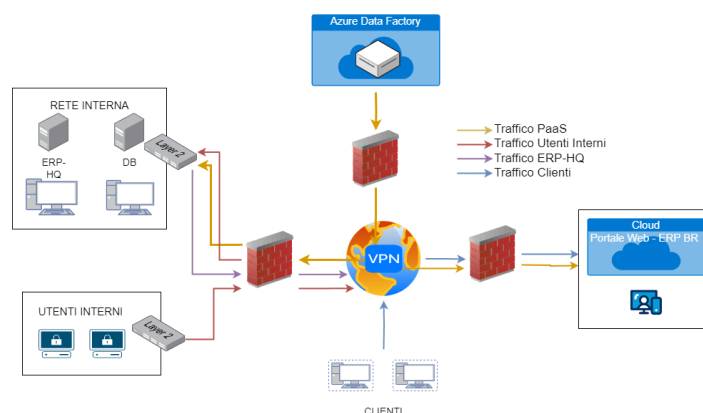
	Network		\$400,001 to \$500,000	On-premise	Database, Information Security, IT Systems Management, Network	Si tratta dell'infrastruttura aziendale comprese le misure di sicurezza e dispositivi di rete.	Opzione 2
	Personale		\$900,001 to \$1,000,000	On-premise		L'organizzazione ha una sede centrale e molte filiali. Di conseguenza si ipotizza che il costo del personale sia ingente.	Opzione 2
	Portale Web		\$400,001 to \$500,000	Cloud	Collaboration	Il portale Web dell'ERP-BR è appaltato e gestito dal provider al quale si affida la nostra organizzazione.	Opzione 2

6. Architettura di rete

6.1 - Analisi dell'architettura

Soluzione PaaS in Cloud

Si è scelto di sostituire il middleware con **ADF (Azure Data Factory)** che è una soluzione iPaaS, che offre un servizio per l'estrazione, caricamento, trasformazione e trasferimento dei dati basato su cloud Azure. Quindi, sostituisce il ruolo del modulo covert permettendo il **trasferimento dei dati da un sistema gestionale all'altro**.



In particolare, ADF permette di eseguire una serie di operazioni come unione, filtraggio, aggregazione e trasformazioni personalizzate, per preparare i dati per l'analisi o il caricamento in una destinazione senza problemi legati alla compatibilità delle singole fonti dati.

Inoltre, Azure Data Factory offre funzionalità di automazione avanzate che consentono all'azienda di pianificare e eseguire automaticamente i flussi di lavoro di integrazione dei dati in base a trigger temporali o eventi specifici. Ciò consente all'azienda di automatizzare i processi di integrazione dei dati, riducendo il carico di lavoro manuale e aumentando l'efficienza operativa. In aggiunta, sono integrati anche sistemi di monitoraggio e gestione dell'andamento

dei flussi di lavoro che consentono di identificare eventuali anomalie e ottimizzarne immediatamente le prestazioni.

La soluzione scelta incontra le esigenze aziendali anche dal punto di vista del **no-code**. Infatti, la funzionalità **Mapping Data Flows** permette la trasformazione dei dati senza la necessità di scrivere codice, rendendo il processo accessibile anche a chi non ha competenze di programmazione avanzata. Utilizzando gli strumenti drag-and-drop di ADF, i dipendenti dell'organizzazione possono definire facilmente i mapping dei dati, associando i campi di dati tra le fonti dati e le destinazioni senza la necessità di scrivere codice SQL o script.

Azure Data Factory fornisce, inoltre, diverse funzionalità di sicurezza, tra cui l'integrazione con Azure Active Directory per l'autenticazione e l'autorizzazione, la crittografia dei dati a riposo e in transito e il controllo degli accessi basato sui ruoli (RBAC) per gestire l'accesso ai dati e alle pipeline.

Essendo un servizio PaaS, la responsabilità del software intermediario e del relativo database è esclusivamente a carico del provider del servizio, Microsoft, liberando l'organizzazione dalla manutenzione di hardware e l'aggiornamento di OS e dalla gestione del software.

In conclusione, tramite ADF, l'organizzazione ha il controllo completo sul mapping delle strutture dati e sulla configurazione delle attività di integrazione, e i suoi dipendenti sono in grado di definire e gestire autonomamente i mapping dei dati senza fare affidamento su terze parti o sviluppatori esterni, grazie alla natura no-code di ADF.

6.2 - Note Finali

L'architettura di rete garantisce la separazione dei servizi interni da quelli degli utenti, limitando l'accesso e migliorando la sicurezza. La VPN (virtual private network) viene implementata per le comunicazioni sicure tra ADF, ERP-HQ ed ERP-BR, mentre il portale web fornisce l'interfaccia per i clienti senza esporre direttamente l'infrastruttura interna. L'implementazione di firewall, IDS/IPS e aggiornamenti regolari aumenta la sicurezza complessiva del sistema. Per migliorare la continuità operativa, si dovrebbe considerare l'implementazione di soluzioni aggiuntive come backup regolari e disaster recovery.

6.3 - Politiche di Accesso

- **Utenti Interni:** Accesso completo all'ERP-HQ, con accesso diretto a internet ma non all'ERP-BR
- **ERP-HQ:** Può collegarsi ad internet per aggiornamenti software, e non per comunicare con ERP-BR.
- **Middleware:** Unico punto di connessione tra ERP-HQ e ERP-BR tramite VPN
- **Clienti:** Accesso al portale web dell'ERP-BR per interagire con i servizi che offre l'azienda.