UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

"REVISIONE DI UN SISTEMA DI ROLE BASED ACCESS CONTROL"

Relatore: Prof. Migliardi Mauro

Laureando: Merotto Alberto

ANNO ACCADEMICO 2021 - 2022
Data di laurea 17/03/2022

Sommario

A seguito degli scandali finanziari degli anni 2000 (e.g. Enron, Parmalat) e della sfiducia nel mercato che hanno generato, i governi hanno deciso di definire delle regole per proteggere gli investitori. Ogni stato, a partire dagli Stati Uniti, ha definito delle proprie leggi a riguardo che mirano specificatamente a:

- Responsabilizzare le società sulle tematiche di accountability e relazioni finanziarie;
- Aumentare le pene dovute a crimini o illeciti contabili.

La normativa apripista, quella degli Stati Uniti, è la Sarbanes and Oxley act proposta dal deputato Oxley e dal senatore Sarbanes, appunto, e comunemente conosciuta come SOX. In Italia le normative di riferimento sono la legge 262/2005 (Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari) ed il decreto legislativo 231/2001 (Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300).

Questo elaborato tratta del caso che ho seguito durante il mio tirocinio svoltosi tra giugno e dicembre 2021 presso Accenture S.p.A., multinazionale di consulenza informatica. Il cliente che ho seguito è un'azienda leader nel settore del food & beverage mondiale che attualmente usa il sistema SAP come ERP per la gestione aziendale. Il sistema in questione verrà aggiornato alla versione S/4 Hana e, in questo passaggio, si è deciso di rivedere i profili degli utenti in modo da fare pulizia dei ruoli non usati e rendere i profili il più possibile immuni dai rischi di tipo SoD (Segregation of Duties).

Indice

1 | Introduzione

1.1 Enterprise Resource Planning – ERP

Un Enterprise Resource Planning (ERP) è un sistema di gestione aziendale che integra tutti i principali processi di business, spesso gestito in real time e realizzato mediante l'utilizzo di software e tecnologia. Un ERP è spesso indicato come una categoria di software di gestione aziendale, tipicamente una suite di applicazioni integrate, che un'organizzazione può utilizzare per raccogliere, archiviare, gestire ed interpretare i dati da varie attività aziendali. I sistemi ERP possono essere locali o basati su cloud. Le applicazioni basate su cloud sono cresciute negli ultimi anni a causa della disponibilità di informazioni da qualsiasi luogo con accesso a Internet. Un ERP mette a disposizione una visione di insieme dei processi core dell'azienda costantemente aggiornata mediante l'utilizzo di basi di dati tradizionali gestite da un database management system (DBMS). I sistemi ERP tengono traccia delle risorse aziendali, dalle materie prime allo stato degli impegni commerciali: ordini, ordini di acquisto e buste paga. Le applicazioni che compongono il sistema condividono i dati tra i vari reparti (produzione, acquisti, vendite, contabilità, ecc.).

Quella degli ERP è un'industria multimiliardaria che produce componenti a supporto di una varietà di funzioni aziendali. I primi ERP erano destinati alle grandi imprese mentre ora sempre più piccole e medie imprese cominciano ad utilizzare un sistema di ERP.

1.2 Caratteristiche e aree funzionali di un ERP

I sistemi ERP tipicamente includono le seguenti caratteristiche:

- Un sistema integrato;
- Operatività in real time (o quasi);
- Un database comune che include tutte le piattaforme;
- Un design e una grafica consistente nei vari moduli.

Mentre invece le aree funzionali che interessano un ERP, e spesso vengono definiti moduli, sono le seguenti:

- Contabilità finanziaria;
- Gestione contabile;
- Ricerca e sviluppo;
- Risorse umane;
- Produzione;
- Elaborazione degli ordini;
- Gestione della supply chain;
- Project management;
- Customer Relationship management (CRM);
- Supplier Relationship Management (SRM);
- Servizi di gestione dati;
- Gestione di istituti scolastici e educativi.

Figura 1.1 Moduli disponibili in un ERP

1.3 Connessione con il reparto di produzione

I sistemi ERP hanno una connessione in tempo reale con i dati e le loro transazioni. La configurazione di questi sistemi viene tipicamente effettuata dai cosiddetti "system integrator", professionisti che possiedono una conoscenza tecnica elevata. Essa può avvenire in diversi modi:

- Integrazione diretta: i sistemi ERP sono dotati di connettività (comunicazione con le apparecchiature di base dell'impianto) come parte della loro offerta di prodotti. Ciò richiede che i fornitori offrano un supporto specifico per le apparecchiature del reparto di produzione dell'impianto con i quali i loro clienti operano;

- Integrazione del database: i sistemi ERP si collegano alle sorgenti di dati dell'impianto tramite delle staging table[1] in un database. Il reparto di produzione deposita le informazioni necessarie all'interno del database, successivamente vengono letti dal sistema ERP. Il vantaggio di questa opzione è che i system integrator non devono specializzarsi anche nel funzionamento delle apparecchiature del reparto di produzione, la loro responsabilità è la connessione;

[1]Le staging table sono che tabelle vengono create utilizzando un database relazionale per organizzare i dati in un formato che può essere facilmente abbinato all'applicazione.

- Enterprise appliance transaction modules (EATM): questi dispositivi comunicano direttamente con il reparto di produzione e con il sistema ERP con i metodi concessi dal sistema ERP. Un EATM può utilizzare una staging table, servizi web oppure delle API specifiche. Un EATM rappresenta una soluzione off-the-shelf[2];

- Soluzioni di integrazioni custom: molti system integrator offrono soluzioni custom. Queste hanno il costo iniziale più elevato e possono avere anche il più alto costo di manutenzione a lungo termine.

1.4 Implementazione

La fase di implementazione solitamente implica modifiche significative al modo di lavorare degli impiegati, inclusi i processi e le pratiche. Generalmente, vengono offerti tre tipi di servizi per implementare tali modifiche: consulenza, personalizzazione e supporto. La durata della fase di implementazione dipende dalla grandezza dell'azienda, il numero di moduli, la personalizzazione, la grandezza dello scope delle modifiche ai processi, e la capacità e prontezza del cliente di prendere padronanza del progetto. I moduli del sistema possono venire implementati in diversi step, rendendo così graduale la transizione. Un tipico progetto per una grossa azienda richiede circa 14 mesi e 150 consulenti, dove la personalizzazione dell'implementazione può incrementare sostanzialmente il tempo necessario.

Spesso l'implementazione del sistema ERP richiede delle modifiche nel processo aziendale ed è quindi fondamentale che le organizzazioni analizzino meticolosamente i vari step del processo prima di rilasciare il software di ERP. La configurazione del sistema è poi sostanzialmente una questione di bilanciare come l'azienda vuole che funzioni il sistema con il modo di funzionare con il quale era stato inizialmente pensato il sistema.

[2]Una soluzione off-the-shelf rappresenta una soluzione pronta all'uso, sviluppata per un mercato di massa che quindi deve soddisfare le necessità di più categorie di utenti possibili.

I moderni sistemi di ERP possono essere implementati in diversi modi: in un cloud pubblico o privato, on premise[3] o in vari scenari ibridi che combinano gli ambienti.

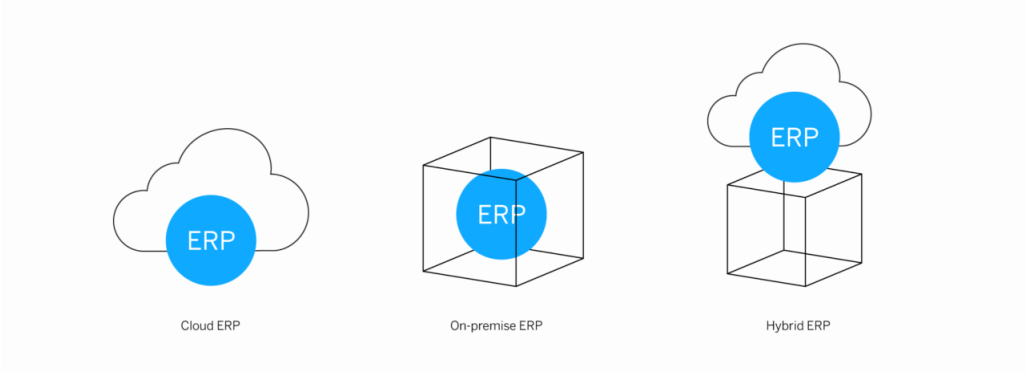


Figura 1.2 Possibili implementazioni di un sistema ERP

1.5 Vantaggi

Il principale vantaggio fornito da un ERP è che l'integrazione di una notevole quantità di processi aziendali fa risparmiare tempo e denaro. È quindi possibile per i dirigenti prendere delle decisioni più velocemente commettendo meno errori e tutti i dati sono visibili trasversalmente all'interno dell'azienda. In particolare, si riscontrano dei benefici nelle seguenti aree:

- Ottimizzazione dell'inventario;
- Cronologia storica di ogni transazione;
- Tracciamento degli ordini;
- Tracciamento dei guadagni;
- Correlazione tra ordini di acquisto, ricevute dell'inventario e spese effettuate;

[3]On premise significa che il sofware è installato e viene eseguito direttamente nelle macchine locali interne all'azienda

- Allineamento dei dati tra tutti gli utenti del sistema;
- Protegge i dati riservati;
- Legittimità e trasparenza ai dati statistici.

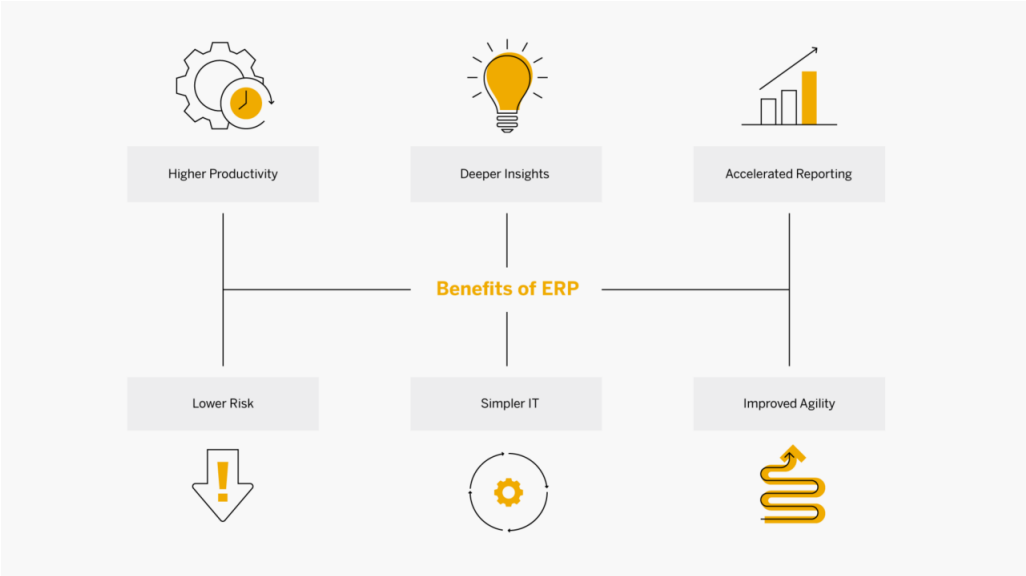


Figura 1.3 Vantaggi di un sistema ERP

1.6 Svantaggi

Inevitabilmente con l'apporto di una modifica così sostanziale al modo di lavorare di tutti i giorni ci possono essere degli inconvenienti e si potrebbe dover scendere a compromessi. Tra i principali svantaggi di un sistema di ERP troviamo:

- Difficoltà nell'adeguamento e nella personalizzazione possono costringere l'azienda a trovare dei compromessi per venire incontro a esigenze specifiche;
- La reingegnerizzazione dei processi aziendali potrebbe danneggiare la competitività dell'azienda oppure distogliere l'attenzione da altre attività fondamentali;

- Un sistema ERP potrebbe costare molto di più rispetto a soluzioni meno integrative o meno complete;
- Alti costi di commutazione ERP possono aumentare il potere negoziale del fornitore ERP, che può aumentare le spese di supporto, manutenzione e aggiornamento;
- L'integrazione di imprese veramente indipendenti può creare dipendenze inutili;
- Le ampie esigenze di formazione prendono risorse dalle operazioni quotidiane;
- L'armonizzazione di un sistema ERP richiede molto tempo, pianificazione e denaro.

1.7 SAP ERP - Ruoli e autorizzazioni

Un esempio di ERP è il sistema SAP, il quale è attualmente in uso presso il cliente da me seguito. All'interno del sistema SAP le autorizzazioni vengono raggruppate all'interno dei ruoli e i ruoli vengono assegnati agli utenti. Le autorizzazioni offrono la possibilità di limitare la visualizzazione e/o la modifica delle informazioni. Il proprietario delle informazioni è responsabile delle decisioni di chi può avere accesso alle informazioni.

Ad un utente possono essere assegnati diversi ruoli. All'interno di ogni ruolo sono presenti degli oggetti che contengono ai quali sono agganciati dei field name che possono essere valorizzati in diverso modo. Quando all'interno del ruolo è presente l'oggetto '`S_TCODE`' e contiene il field name '`TCD`', i valori autorizzativi vengono definiti 'Transazioni'. Le transazioni servono ad accedere a determinate funzioni in SAP in maniera diretta e sono quindi trattate con un occhio di riguardo. La struttura di un ruolo può quindi essere così visualizzata:

Role	Object	Field name	Authorization value FROM	Authorization value TO
ROLE01	S_TCODE	TCD	XX	
ROLE01	OBJ_01	FLD_XX	*	
ROLE01	OBJ_02	FLD_XY	*	
ROLE01	OBJ_02	FLD_XZ	*	
ROLE01	OBJ_03	FLD_XI	01	
ROLE01	OBJ_03	FLD_XJ	*	
ROLE01	OBJ_04	FLD_XL	*	
ROLE01	OBJ_05	FLD_XK	24	
ROLE01	OBJ_05	FLD_XM	*	
ROLE01	OBJ_05	FLD_XP	*	
ROLE01	OBJ_05	FLD_XQ	*	
ROLE02	OBJ_05	FLD_XQ	*	
ROLE02	OBJ_05	FLD_XP	*	
ROLE02	OBJ_03	FLD_XK	03	
ROLE02	OBJ_03	FLD_XJ	*	
ROLE02	OBJ_03	FLD_XI	015	030
ROLE02	OBJ_02	FLD_XZ	*	
ROLE02	OBJ_02	FLD_XY	*	
ROLE02	OBJ_01	FLD_XX	*	
ROLE02	S_TCODE	TCD	XX	
ROLE03	OBJ_05	FLD_XQ	*	
ROLE03	OBJ_05	FLD_XP	*	
ROLE03	OBJ_05	FLD_XM	*	
ROLE03	OBJ_05	FLD_XK	25	50
ROLE03	OBJ_04	FLD_XL	*	
ROLE03	OBJ_02	FLD_XZ	*	
ROLE03	OBJ_02	FLD_XY	*	
ROLE03	OBJ_01	FLD_XX	*	
ROLE03	S_TCODE	TCD	XX	
ROLE04	S_TCODE	TCD	XZ	
ROLE04	S_TCODE	TCD	XS	
ROLE04	S_TCODE	TCD	XP	
ROLE04	S_TCODE	TCD	XQ	

Figura 1.4 La struttura di un ruolo

1.8 La gestione della sicurezza

La gestione della sicurezza di un sistema SAP da parte di Accenture individua cinque livelli che vanno controllati:

1. Livello organizzativo, formato da:

   (a) Consapevolezza: ogni utente deve essere formato ad un minimo livello di conoscenza che consenta di contribuire alla sicurezza totale

del sistema;

(b) Governance della sicurezza: l'obiettivo è di definire le responsabilità di tutte le parti coinvolte tramite i ruoli;

(c) Gestione dei rischi: comprende tutta la parte di identificazione, gestione, mitigazione e risoluzione dei rischi.

2. Livello di processo:

   (a) Conformità alla normativa: se non usate correttamente le funzioni dell'applicativo possono violare considerevolmente i requisiti legali;

   (b) Privacy e protezione dei dati: stabilire e mantenere una configurazione sicura per le applicazioni di business custom e standard;

   (c) Attività di audit e gestione delle frodi: assicurare e verificare la conformità dell'infrastruttura e delle operazioni IT con le linee guida interne ed esterne.

3. Livello applicativo:

   (a) Gestione delle utenze e delle identità: definizione e implementazione di utenze IT incluse utenze speciali e amministratori; definizione di un corretto schema delle autorizzazioni utilizzando le regole della Segregation of Duties (SoD);

   (b) Autenticazione e Single Sign-On: il Single Sign-On è una soluzione per l'autenticazione; implementazione di meccanismi appropriati di singol o multi-factor authentication;

   (c) Ruoli e autorizzazioni: gestione degli accessi in visualizzazione e modifica alle informazioni; gestione e mitigazione dei rischi generati secondo le regole SoD. Una segregazione custom può essere implementata per incontrare le necessità del cliente;

   (d) Sicurezza del codice custom: l'obbiettivo è quello di proteggere il sistema SAP da codice malevolo, il quale può essere contenuto in ogni tipo di codice processato da SAP (e.g. Cross Site Scripting, SQL injection).

4. Livello di sistema:

   (a) Sicurezza avanzata: tratta principalmente di sicurezza su misura di parametri rilevanti di sistema e altre configurazioni; tratta anche di componenti frontend di SAP come ad esempio la SAP GUI;

   (b) Sicurezza del codice di SAP: mantenimento della sicurezza del codice SAP tramite l'applicazione delle patch di sicurezza più recenti;

   (c) Monitoraggio della sicurezza e analisi forense: revisione e monitoraggio regolare della sicurezza del sistema SAP sulla base di un setup sicuro.

5. Livello di ambiente:

   (a) Sicurezza della rete: mantenimento di un'appropriata topologia della rete, segregazione e dominio. Limitazione dei servizi di rete e dei protocolli;

   (b) Sistema operativo e sicurezza del database: le misure di sicurezza di base del sistema operativo devono essere attive e funzionanti; nell'accedere al database preferire gli strumenti officiali forniti da SAP;

   (c) Sicurezza del client: stabilire un'adeguata sicurezza del front-end incluse le workstation e i dispositivi mobili.

Il mio lavoro si è principalmente focalizzato sulla sicurezza a livello applicativo, in particolare nell'analisi dei ruoli già presenti a sistema, al miglioramento di essi e alla creazione di nuovi, in modo da fornire al cliente un set di ruoli sicuri e affidabili che saranno assegnati agli utenti nel passaggio alla nuova versione S4/Hana.

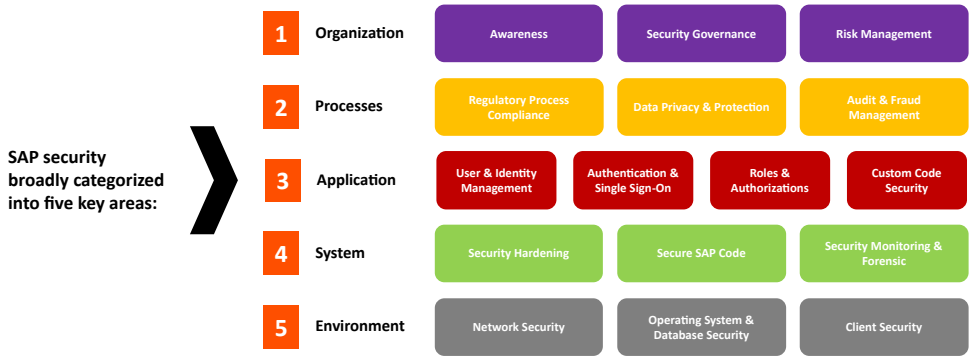


Figura 1.5 Organizzazione della sicurezza di un sistema SAP

1.9 L'importanza della sicurezza

In un'ottica aziendale la sicurezza del sistema SAP è fondamentale in quanto minimizza il rischio che avvengano truffe e/o frodi. Tramite, infatti, l'applicazione di importanti principi, quali la "Segregation of Duties", "Least privileges" e "Need to know" le azioni degli utenti a sistema diventano limitate al loro ruolo in azienda così da non permettere l'esecuzione di azioni potenzialmente rischiose se eseguite da una stessa persona. Ne è un esempio il ciclo passivo di fatturazione: il concetto di ciclo passivo infatti riguarda tra gli altri fattori le voci di spesa dell'azienda, tra cui i pagamenti. Se un utente fosse quindi contemporaneamente in grado di inserire un pagamento, modificare l'anagrafica del fornitore o addirittura inserirne una nuova ed approvare il pagamento stesso, potrebbe commettere una truffa effettuando il pagamento verso un qualsiasi IBAN.

2 | Principi di sicurezza

Nel campo della sicurezza informatica il termine CIA è l'acronimo di confidentiality, integrity, and availability, ovvero riservatezza, integrità e disponibilità.

Questi tre principi formano, insieme, la base dell'infrastruttura di sicurezza di qualsiasi organizzazione. Essi sono quello che dovrebbe essere l'obiettivo della messa in sicurezza di un qualunque sistema aziendale e sono così importanti che ogni volta che vi è una fuga di dati, un sistema viene attaccato, un utente è vittima di un attacco di phishing, un account viene dirottato, un sito web viene maliziosamente rimosso, o si verifica un qualunque altro attacco alla sicurezza, significa che almeno uno di questi principi è stato violato.

Figura 2.1 La triade CIA

In particolare, questa triade si occupa nello specifico di:

- **Riservatezza**: si riferisce agli sforzi di un'azienda di mantenere i propri dati privati e segretati. Nella pratica questo si traduce nel controllare l'accesso ai dati per impedire la divulgazione non autorizzata delle informazioni. In genere, ciò implica garantire che solo coloro che sono autorizzati abbiano accesso a risorse specifiche e che coloro che non sono autorizzati siano attivamente impediti di ottenere l'accesso.

  Ad esempio nella gestione del meccanismo di payroll, solo i dipendenti autorizzati dovrebbero avere accesso al database dei salari dei dipendenti.

  Le contromisure per proteggere la riservatezza comprendono la classificazione e l'etichettatura dei dati; forti controlli di accesso e meccanismi di autenticazione; crittografia dei dati nella fase di processo, in quella di transito e in quella di deposito; capacità di cancellazione remota; infine un'istruzione e una formazione adeguate per tutte le persone con accesso ai dati;

- **Integrità**: si riferisce alla capacità del sistema di essere corretto, autentico e affidabile. In particolare, che i dati che vengono acceduti non siano stati manomessi e siano quindi affidabili. Per esempio, i clienti di una banca devono potersi fidare che le loro informazioni bancarie e i saldi dei loro conti non siano stati manomessi.

  Le contromisure che proteggono l'integrità dei dati includono la crittografia, l'hashing, le firme digitali, i certificati digitali (le autorità di certificazione (CA) rilasciano certificati digitali alle organizzazioni per verificare la loro identità agli utenti del sito web, simile al modo in cui il passaporto o la patente di guida possono essere utilizzati per verificare l'identità di un individuo), sistemi di rilevamento delle intrusioni, auditing, controllo di versione e forti meccanismi di autenticazione e controlli di accesso;

- **Disponibilità**: le funzionalità e le applicazioni software di un sistema diventano di scarsa importanza se il sistema non è semplicemente ac-

cessibile. La disponibilità indica quindi che le reti, i sistemi e le applicazioni siano caricate e funzionanti. Assicura inoltre che gli utenti autorizzati abbiano accesso tempestivo e affidabile alle risorse quando necessario. Molte cose possono compromettere la disponibilità, tra cui guasti hardware o software, mancanza di corrente, disastri naturali ed errori umani. Da segnalare inoltre per quanto riguarda gli attacchi malevoli è l'attacco 'denial-of-service', in cui le prestazioni di un sistema, sito web o applicazione web-based sono intenzionalmente e maliziosamente degradate e in alcuni casi il sistema potrebbe diventare completamente irraggiungibile. Le contromisure per garantire la disponibilità includono ridondanza (in server, reti, applicazioni e servizi), tolleranza dei guasti hardware (per server e dispositivi di archiviazione), patch software regolari e aggiornamenti di sistema, backup e soluzioni di protezione all'attacco di 'denial-of-service'.

Due principi che aiutano a garantire la conformità CIA di un sistema e che sono stati utilizzati nella realizzazione e personalizzazione dei ruoli per gli utenti della società del cliente sono i principi di 'Least Privilege' e 'Need to Know'.

2.1 La Segregation of Duties - SOD

Lo scopo della Segregation of Duties (SoD) è di assicurare che solo persone considerate idonee possano eseguire transazioni considerate "sensitive". È quindi necessario segmentare il processo così che un utente non presenti un rischio di frode.

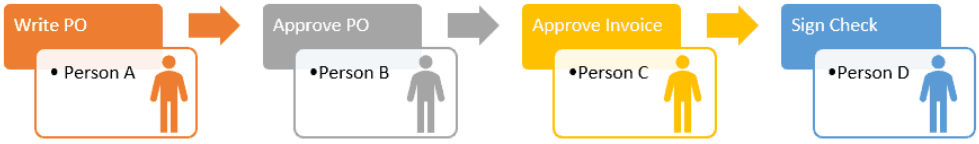


Figura 2.2 Esempio di Segregation of Duties

Un modello da noi adottato per la gestione della SoD necessita di due librerie:

- La libreria dei duties, che sono famiglie di transazioni (business action di SAP, e.g. modifica ai dati materiali, creazione di un ordine di acquisto);
- La libreria dei rischi, cioè i duties in conflitto tra di loro.

Un duty (o function) rappresenta un certo set di transazioni che costituiscono la parte di un processo.

La libreria dei rischi definisce le parti di processo che sono in conflitto tra di loro.

I termini utilizzati nella gestione della segregation of duties sono i seguenti:

- *Ruleset o array*: rappresenta il set dei rischi o delle regole;
- *Processo*: identifica un set di task;
- *Rischio*: insieme formato da due o più function in conflitto tra loro;
- *Function*: rappresenta un insieme di attività che formano un processo aziendale;

- *Action/Permission*: sono il dettaglio tecnico delle attività (transazioni) ed oggetti autorizzativi (permission) usati nell'ambiente SAP per poter svolgere operazioni di business a sistema;

- *Controlli compensativi*: sequenza di azioni utilizzata per verificare e controllare le evidenze reali di rischio.

È necessario quindi quando si effettua un'analisi SoD definire una matrice (o ruleset) che identifichi i rischi e le function per tutte le transazioni sia standard che custom.

Risk	Function 1	Function 2	Function 3	Function 4	Function 5	Priority	Active Vs Not Active	Risk Type
ZSODXX01	ZXX02	ZXX03				0	0	1
ZSODXX02	ZXX04	ZXX05				0	0	1
ZSODXY01	ZXY01	ZXY03				0	0	1
ZSODXY02	ZXY03	ZXY04				0	0	1
ZSODXY03	ZXY01	ZXY04				0	0	1
ZSODXY04	ZXY02	ZXY05				0	0	1
ZSODXY05	ZXY01	ZXY05				0	0	1
ZSODXY06	ZXY02	ZXY04				0	0	1
ZSODXZ01	ZXZ02	ZPP03				0	0	1
ZSODXZ02	ZXZ01	ZXZ02				0	0	1
ZSODXZ03	ZXZ02	ZXZ04				0	0	1

Figura 2.3 Esempio di matrice dei rischi

Un rischio viene quindi generato nel momento in cui un utente possiede contemporaneamente due o più function che si possono trovare sia all'interno dello stesso ruolo oppure in ruoli diversi.

Una function è composta da diverse action, che corrispondono alle transazioni del ruolo. Se un utente possiede quindi almeno una transazione tra le action della function egli potrebbe avere tale function. Per la conferma definitiva bisogna controllare che l'utente possieda tutti i permission (che corrispondono agli 'object' dei ruoli) e che siano valorizzati allo stesso modo, quindi abbiano gli stessi Field, Authorization Value (tutti quanti se indicati in AND nella matrice o almeno uno se indicati come OR nella matrice) all'interno dei suoi ruoli.

Function	Action	Permission	Field	Authorization Value From	Authorization Value To	Operator AND/OR/NOT	Active VS Not Active
XX01	AA01	PRM_A	FLD_A	01	02	AND	0
XX01	AA02	PRM_A	FLD_A	01	02	AND	0
XX01	AA03	PRM_A	FLD_A	01	02	AND	0
XX01	AA04	PRM_A	FLD_A	01	02	AND	0
XX01	AA05	PRM_B	FLD_B	31		OR	0
XX01	ACT06	PRM_B	FLD_B	26		OR	0
XX01	ACT06	PRM_B	FLD_B	25		OR	0
XX01	ACT06	PRM_B	FLD_B	24		OR	0
XX01	ACT06	PRM_B	FLD_B	21		OR	0
XX01	ACT06	PRM_B	FLD_B	15		OR	0
XX01	ACT06	PRM_B	FLD_B	14		OR	0
XX03	ACT07	PRM_C	FLD_B	02		AND	0
XX03	ACT08	PRM_D	FLD_B	01	02	AND	0
XX03	ACT09	PRM_D	FLD_B	85		OR	0
XX03	ACT10	PRM_D	FLD_B	01		OR	0
XX03	ACT11	PRM_D	FLD_B	02		AND	0
XY02	ACT12	PRM_E	FLD_B	01	02	AND	0
XY02	ACT13	PRM_E	FLD_B	01	02	AND	0
XY02	ACT14	PRM_E	FLD_B	01	02	AND	0
XY02	ACT15	PRM_E	FLD_B	01	02	AND	0
XY02	ACT16	PRM_E	FLD_B	01	02	AND	0
XY02	ACT17	PRM_E	FLD_B	01	02	AND	0
XY02	ACT18	PRM_E	FLD_B	01	02	AND	0
XY02	ACT19	PRM_E	FLD_B	01	02	AND	0
XY02	ACT20	PRM_E	FLD_B	01	02	AND	0
XY02	ACT21	PRM_E	FLD_B	01	02	AND	0
XY02	ACT22	PRM_E	FLD_B	01	02	AND	0

Figura 2.4 Esempio di matrice delle functions

La Risk Analysis

Una volta quindi definita la matrice SoD è possibile effettuare la Risk Analysis, cioè un'analisi degli utenti presenti a sistema che evidenzia quali rischi SoD essi generano. Per quest'analisi, SAP mette a disposizione il tool GRC (Governance, Risk and Compliance) che permette di ottenere un output di tutti i rischi attivati dagli utenti e i loro dettagli.

Nella figura 2.5 è possibile visualizzare un esempio di output dei rischi a livello intra-ruolo. Infatti, anche i ruoli stessi posso contenere al loro interno delle function che possono quindi attivare dei rischi.

Una volta ottenuto il risultato della risk analysis è possibile procedere con la fase di risoluzione e mitigazione dei rischi.

Questa fase ha inizio con la rimozione di tutto ciò che non è mai stato utilizzato o non viene utilizzato da molto tempo, poiché magari alcune parti di processo sono state modificate oppure degli utenti hanno cambiato mansione, e spesso porta già ad un abbattimento considerevole dei rischi evidenziati in

Role Name	Comment	Access Risk ID	Risk Description	Rule ID	Risk Level	System	Action	Action Description
Role01	No Violations					SYST01	No Violations	
Role02	No Violations					SYST01	No Violations	
Role03	No Violations					SYST01	No Violations	
Role04	No Violations					SYST01	No Violations	
Role05	No Violations					SYST01	No Violations	
Role06	No Violations					SYST01	No Violations	
Role07	Comment01	RISKXX001	Description 01	00X	Medium	SYST01	ACT01	ActDsc01
Role07	Comment02	RISKXX001	Description 01	00X	Medium	SYST01	ACT02	ActDsc02
Role07	Comment03	RISKXY01	Description 02	00Y	Medium	SYST01	ACT03	ActDsc03
Role07	Comment03	RISKXY01	Description 02	00Y	Medium	SYST01	ACT04	ActDsc04
Role07	Comment03	RISKXY02	Description 03	00Z	Medium	SYST01	ACT05	ActDsc05
Role07	Comment03	RISKXY02	Description 03	00Z	Medium	SYST01	ACT04	ActDsc06
Role07	Comment03	RISKXY02	Description 03	00I	Medium	SYST01	ACT04	ActDsc06
Role07	Comment03	RISKXY02	Description 03	00J	Medium	SYST01	ACT04	ActDsc06
Role07	Comment03	RISKXY02	Description 03	00J	Medium	SYST01	ACT05	ActDsc07
Role07	Comment03	RISKXY02	Description 03	00K	Medium	SYST01	ACT04	ActDsc06

Figura 2.5 Esempio di output di risk analysis a livello intra-ruolo

una prima analisi.

Successivamente è necessario apportare delle modifiche di fino ai ruoli e per fare ciò si ha una forte interazione con gli utenti business, con i quali si cerca di capire come possano essere risolti i rischi. Questa fase può richiedere molto tempo e lunghe analisi per giungere a compimento ma è necessaria al fine di non bloccare il lavoro degli utenti una volta che le modifiche saranno apportate.

Una volta terminata questa analisi la maggior parte dei rischi sarà quindi stata rimossa, mentre ci possono essere dei rischi che rimangono attivi poiché non si è riusciti a segmentare sufficientemente il processo per varie ragioni (e.g. carenza di personale addetto a quella parte di processo) e tali rischi vengono quindi accettati e devono essere mitigati.

La fase di mitigazione prevede la messa in uso di controlli compensativi sulle azioni degli utenti a rischio SoD, controlli custom che tengano monitorata l'attività di questi utenti con un occhio di riguardo a quelle che possono essere attività potenzialmente rischiose.

2.2 Least Privilege

Il principio di Least Privilege serve ad indirizzare la tematica del controllo degli accessi e afferma che un utente dovrebbe avere solamente il minimo dei

permessi di accesso necessari per svolgere un compito e portarlo a termine e nulla di più. Quindi per esempio un dipendente il cui compito è quello di gestire le buste paga non dovrà avere accesso al database amministrativo del cliente. Parallelamente, uno specialista di marketing, per svolgere il suo lavoro non dovrà avere accesso ai dati dei salari dei dipendenti.

Questo meccanismo ci risulta familiare se pensiamo a delle situazioni che possono capitare ogni giorno, come ad esempio il parental control applicato dai genitori per impedire ai bambini l'accesso a contenuto dannoso oppure gli studenti che hanno accesso alla piattaforma di e-learning ma solo ai file a loro concessi e non ai file interni dei docenti.

L'obiettivo è quindi quello di ridurre al minimo tutti i danni derivanti da un'eccessiva concessione dei privilegi e del loro scorretto utilizzo, sia accidentalmente che maliziosamente. Il principio di Least Privilege si applica non solo però agli utenti intesi come individui ma anche alle reti, dispositivi, programmi e servizi. Quando infatti si parla di controllo degli accessi tutti questi vengono considerati come entità attive poiché esse richiedono l'accesso ai dati. È quindi fondamentale per un'azienda comprendere come questo principio vada applicato a tutte queste entità perché, se non implementato correttamente, ognuna di esse potrebbe metterla a rischio ed esporre i suoi dati.

Sebbene il Least Privilege sia uno dei principi di sicurezza più di buon senso, spesso le aziende non lo prendono seriamente e mancano di implementarlo correttamente. Con riferimento infatti alla triade CIA, un sistema che non implementa correttamente il Least Prvilege può violare tutte e tre le condizioni di riservatezza, integrità e disponibilità. Ad esempio:

- Un impiegato addetto alle buste paga che cancella il database del cliente viola la disponibilità;
- Un addetto alla vendita che vede i dati salariali dei dipendenti viola la riservatezza;
- Uno specialista finanziario che cambia il codice sorgente dell'applicazione viola l'integrità.

Vale la pena inoltre notare come nella OWASP Top Ten[1] i meccanismi impropri o malfunzionanti di autenticazione o controllo degli accessi sono indicati in almeno quattro dei dieci principali rischi di sicurezza delle applicazioni web.

Uno dei maggiori benefici nella corretta applicazione del Least Privilege è quello della riduzione della "attack surface", ovvero tutti i punti di ingresso che un hacker potrebbe sfruttare per ottenere l'accesso al sistema. Avere un'ampia "superficie di attacco" è pertanto difficoltoso e problematico da gestire e può avere conseguenze disastrose nel caso in cui ad esempio vengano attaccati database basati su cloud non protetti, API senza controlli di autenticazione, backdoor (un modo non documentato per accedere a un sistema che consente a un utente malintenzionato di bypassare i controlli di sicurezza tipici) lasciati in software critici, o server aperti a qualsiasi tipo di traffico. A causa di queste mancanze si sono verificati diversi attacchi e di recente abbiamo diversi esempi:

- La violazione dei dati di Capital One del 2019 che ha esposto le informazioni personali di 106 milioni di consumatori era dovuta in parte a un firewall a cui erano stati assegnati privilegi eccessivi, permettendogli di eseguire comandi e accedere ai dati in uno storage cloud a cui non avrebbe dovuto avere accesso;

- Nel 2019 e nel 2020, molteplici violazioni dei dati hanno esposto le informazioni personali di milioni di utenti e, in un caso, di 1.2 miliardi di utenti. In tutti i casi, i database basati su cloud sono stati esposti perché non avevano protezione password o controlli di accesso di qualsiasi tipo;

- La violazione dei dati del 2019 della società di motori di ricerca indiana Justdial ha esposto informazioni personali di oltre 100 milioni di utenti. La violazione è stata attribuita alle API non autenticate che, a loro volta, hanno dato agli attaccanti accesso illimitato alle API del backend dei dati.

[1]La lista delle vulnerabilità più comuni nelle web application

Infine, a seconda del settore o del tipo di attività, molte organizzazioni devono rispettare le leggi e i requisiti normativi, ad esempio in UE si ha il regolamento generale sulla protezione dei dati (GDPR) e il Sarbanes-Oxley Act negli Stati Uniti. Una corretta attuazione e applicazione del principio di Least Privilege aiuta le aziende a raggiungere la conformità normativa e le mette in una posizione migliore per superare un processo di audit.

2.3 Need To Know

Il principio di Least Privilege può essere spesso confuso con il principio di "Need to Know", il quale viene invece utilizzato per fornire accessi più ampi in caso di necessità. Ad esempio, un dipendente governativo con autorizzazione top-secret non dovrebbe avere accesso illimitato a tutti i contenuti top-secret, solo a contenuti che sono direttamente rilevanti per un progetto o un compito specifico che devono eseguire. Tale accesso può anche essere limitato nel tempo.

3 | Strumenti disponibili

Nell'affrontare questo problema in accordo con il cliente è stato adottato un approccio di tipo brownfield, il quale prevede di partire dalla situazione attuale presente a sistema e cercare di rivederla e modificarla per arrivare al risultato desiderato. Si differenzia dall'approccio greenfield nel quale invece si fa "tabula rasa" della situazione attuale a sistema e si ricostruiscono i ruoli da zero. Generalmente, vista la mole di dati da processare e analizzare in questi casi è preferibile adottare un approccio greenfield, ma per le necessità del cliente si è voluti restare su un approccio brownfield.

3.1 Enterprise Appliance Transaction Module - EATM

Quando si parla di transazione verso un sistema ERP è disponibile una soluzione off-the-shelf che è data dall'Enterprise Appliance Transaction Module (EATM). Un EATM è uno strumento usato per il trasferimento dell'equipaggiamento e dello stato dei prodotti dell'impianto di produzione verso un ERP. Un EATM è composto da:

- Componentistica hardware, data dei sistemi solitamente embedded e dedicati a quello specifico compito;
- Software di comunicazione dei dispositivi, i quali supportano i protocolli per l'automazione usati per estrarre i dati;

- Software di comunicazione aziendale, il quale abilita l'interazione con i sistemi aziendali, ne sono un esempio le interfacce per i database relazionali;

- Applicazione di transazione, software configurato per osservare e raccogliere le variabili del dispositivo, formattarle in transazioni richieste e trasferire i risultati in modo sicuro e affidabile ad altri sistemi. L'applicazione transazione risiede nel mezzo tra le comunicazioni dispositivo e le comunicazioni aziendali.

Questo dispositivo serve quindi a mediare l'interazione tra il sistema attuale del reparto di produzione con il sistema di ERP.

Questa soluzione non risulta però percorribile poiché si ferma all'interazione del reparto di produzione appunto, senza dare informazioni sul ruolo e gli accessi degli utenti.

3.2 SAP GRC Suite - Governance Risk and Compliance

Un altro strumento utile questa volta messo a disposizione da SAP direttamente, è la suite GRC. Questa suite fornisce diverse soluzioni applicative mirate a facilitare l'individuazione, risoluzione e mitigazioni dei rischi e la verifica delle conformità. Questa suite comprende vari sistemi, di cui i principali sono:

- SAP GRC Access Control;
- SAP GRC Process Control;
- SAP GRC Risk Management;
- SAP GRC GTS Global Trade Services;
- SAP Audit Management;
- SAP BIS Business Integrity Screening;

- SAP ETD Enterprise Threat Detection;
- SAP Cloud Identity Access Governance.

Non tutti questi sistemi sono dedicati al controllo degli accessi, in particolare troviamo il sistema GRC Access Control che risulta di nostro interesse; esso è composto dai seguenti moduli:

- Access Risk Analysis (ARA), il quale consente di effettuare un'analisi degli accessi e di evidenziare le situazioni di rischio basate sulla matrice dei rischi;
- Emergency Access Management (EAM), il quale permette di gestire degli accessi privilegiati durante le attività quotidiane da parte degli utenti, principalmente ICT o amministratori;
- Business Role Management (BRM), il quale permette di definire una metodologia di creazione dei ruoli tecnici nel sistema, aggiungendo una serie di funzionalità non previste nel profile generator di SAP standard come ad esempio, naming convention, processi approvativi e risk analysis preventive;
- Access Request Management (ARQ), il quale consente di definire dei workflow per la gestione degli accessi. Ad esempio processi: nuove utenze, modifica utenze, blocco utenze. Questo componente può essere collegato all'LDAP[1] aziendale oppure al sistema SAP HR.

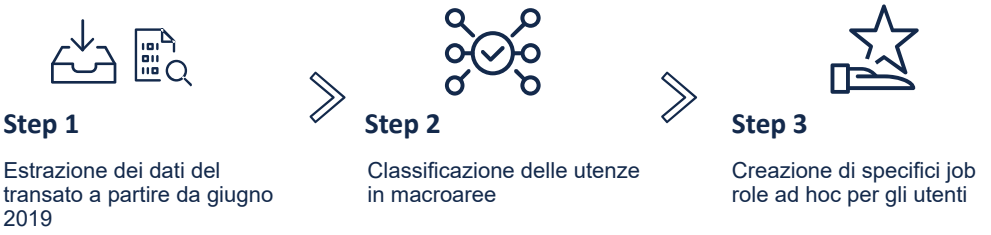
Di queste soluzioni la più inerente è sicuramente il modulo ARA, il quale viene utilizzato appunto per effettuare le risk analysis a valle dell'implementazione dei nuovi ruoli a sistema ed avere quindi visibilità dei rischi presenti.

Per quanto riguarda invece gli altri moduli, l'unico inerente alla creazione dei ruoli e profili è il modulo BRM, che però risulta inutile nel nostro caso in quanto la naming convention era già stata definita da parte del reparto IT

[1]Il Lightweight Directory Access Protocol è un protocollo standard per l'interrogazione e la modifica dei servizi di directory, come ad esempio un elenco aziendale di email o una rubrica telefonica, o più in generale qualsiasi raggruppamento di informazioni che può essere espresso come record di dati e organizzato in modo gerarchico.

del cliente e quindi si è scelto di adottare quella, mentre per quanto riguarda il contenuto dei ruoli la personalizzazione è stata fatta con un lavoro molto più lungo tramite interviste con i responsabili di dipartimento e analisi del transato.

4 | Presentazione della soluzione proposta



4.1 Rimozione dei ruoli non necessari

Nella prima fase, è stato deciso di analizzare il transato di tutti gli utenti per prendere visione di cosa gli utenti stessero e non stessero facendo a sistema. Per fare ciò è stato necessario estrarre dal sistema varie tabelle ed incrociare i dati in esse presenti per ottenere un risultato leggibile ed interpretabile. Il sistema SAP tiene infatti traccia delle azioni effettuate dagli utenti solamente come transazioni nella tabella `GRACACTUSAGE`, le transazioni contenute nei ruoli nella tabella `AGR_1251`[1] mentre i ruoli assegnati agli utenti nella tabella `AGR_USERS`. I dati del transato della tabella `GRACACTUSAGE` sono stati scaricati a partire da giugno 2019, così da avere visione delle attività degli utenti a sistema negli ultimi due anni, avendo iniziato l'analisi a giugno 2021.

[1] la tabella `AGR_1251` tiene in realtà traccia di tutti gli oggetti autorizzativi, i campi e i valori autorizzativi di tutti i ruoli; per accedere alle transazioni bisogna filtrare la tabella con l'oggetto autorizzativo `'S_TCODE'`, il campo `'TCD'` e le transazioni sono quindi date dai valori autorizzativi.

Per poter quindi collegare tutti questi dati tramite la funzione 'Vlookup' di Excel è stato necessario creare prima una chiave nella tabella `GRACACTUSAGE` composta da `'USER NAME - TRANSACTION'`, successivamente tramite l'utilizzo di una tabella pivot sono stati uniti i dati della tabella `AGR_USERS` e della tabella `AGR_1251` in modo da avere il dato delle transazioni associate ad un utente e contemporaneamente i ruoli associati ad esso. A questo punto è stata ricreata la chiave `'USER NAME - TRANSACTION'` e tramite Vlookup si è potuto collegare la data di ultima esecuzione delle transazioni agli utenti e ai ruoli ad essi associati. In questo modo si è potuto verificare quali fossero i ruoli non usati dagli utenti negli ultimi due anni; una volta identificati questi ruoli si è deciso che saranno rimossi nel passaggio alla versione S/4 Hana e quindi per condurre ulteriori analisi di profilazione degli utenti da parte nostra essi non sono più stati considerati.

KEY USER - TCD	User Name	Action	Number of executuions	Last Executed On
001 - TCD01	001	TCD01	7	23/08/2020
006 - TCD13	006	TCD13	1	23/08/2020
006 - TCD14	006	TCD14	1	23/08/2020
006 - TCD15	006	TCD15	4	23/08/2020
007 - TCD16	007	TCD16	1	23/08/2020
008 - TCD17	008	TCD17	7	11/03/2021
009 - TCD18	009	TCD18	1	24/08/2020
010 - TCD19	010	TCD19	2	24/08/2020
011 - TCD20	011	TCD20	22	24/08/2020
012 - TCD21	012	TCD21	11	14/04/2021
013 - TCD22	013	TCD22	1	24/08/2020

Figura 4.1 Estratto della tabella `GRACACTUSAGE`

USER NAME - ROLE	USER NAME - TRANSACTION	User Group	User Name	Full Name	Role	Role Short Description	Transaction	Transaction text
001 - ROLE_A	001 - TCD01	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD01	TCDTXT01
001 - ROLE_A	001 - TCD02	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD02	TCDTXT02
001 - ROLE_A	001 - TCD03	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD03	TCDTXT03
001 - ROLE_A	001 - TCD04	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD04	TCDTXT04
001 - ROLE_A	001 - TCD05	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD05	TCDTXT05
001 - ROLE_A	001 - TCD06	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD06	TCDTXT06
001 - ROLE_A	001 - TCD07	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD07	TCDTXT07
001 - ROLE_A	001 - TCD08	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD08	TCDTXT08
001 - ROLE_A	001 - TCD09	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD09	TCDTXT09
001 - ROLE_A	001 - TCD10	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD10	TCDTXT10
001 - ROLE_A	001 - TCD11	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD11	TCDTXT11
001 - ROLE_A	001 - TCD12	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD12	TCDTXT12
001 - ROLE_A	001 - TCD13	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD13	TCDTXT13
001 - ROLE_A	001 - TCD14	SEMEA-XXXX-X	001	USER A	ROLE_A	ROLE_A - Description A	TCD14	TCDTXT14
002 - ROLE_B	002 - TCD15	SEMEA-XXXX-X	002	USER B	ROLE_B	ROLE_B - Description B	TCD15	TCDTXT15
002 - ROLE_B	002 - TCD16	SEMEA-XXXX-X	002	USER B	ROLE_B	ROLE_B - Description B	TCD16	TCDTXT16
002 - ROLE_B	002 - TCD17	SEMEA-XXXX-X	002	USER B	ROLE_B	ROLE_B - Description B	TCD17	TCDTXT17
002 - ROLE_B	002 - TCD18	SEMEA-XXXX-X	002	USER B	ROLE_B	ROLE_B - Description B	TCD18	TCDTXT18
002 - ROLE_B	002 - TCD19	SEMEA-XXXX-X	002	USER B	ROLE_B	ROLE_B - Description B	TCD19	TCDTXT19
002 - ROLE_B	002 - TCD20	SEMEA-XXXX-X	002	USER B	ROLE_B	ROLE_B - Description B	TCD20	TCDTXT20
002 - ROLE_B	002 - TCD21	SEMEA-XXXX-X	002	USER B	ROLE_B	ROLE_B - Description B	TCD21	TCDTXT21
002 - ROLE_B	002 - TCD22	SEMEA-XXXX-X	002	USER B	ROLE_B	ROLE_B - Description B	TCD22	TCDTXT22
002 - ROLE_B	002 - TCD23	SEMEA-XXXX-X	002	USER B	ROLE_B	ROLE_B - Description B	TCD23	TCDTXT23

Figura 4.2 Estratto della tabella `AGR_1251`

User Name	Full Name	Role	Used	Number of execution	Last Executed On
001	**USER A**	ROLE_A	Used	514	07/06/2021
001	**USER A**	ROLE_B	Used	77	07/06/2021
001	**USER A**	ROLE_C	Used	103	22/02/2021
001	**USER A**	ROLE_D	Used	11	20/05/2021
002	**USER B**	ROLE_E	Used	14	26/01/2021
002	**USER B**	ROLE_F	Used	14	26/01/2021
002	**USER B**	ROLE_G	Used	14	26/01/2021
002	**USER B**	ROLE_H	Used	14	26/01/2021
002	**USER B**	ROLE_I	Used	2	08/01/2020
002	**USER B**	ROLE_J	Used	2	08/01/2020
002	**USER B**	ROLE_K	Used	2	08/01/2020
002	**USER B**	ROLE_L	Used	2	08/01/2020
002	**USER B**	ROLE_M	Used	37	27/05/2021
002	**USER B**	ROLE_N	Used	37	27/05/2021
002	**USER B**	ROLE_O	Used	37	27/05/2021
002	**USER B**	ROLE_P	Used	37	27/05/2021
002	**USER B**	ROLE_Q	Used	37	25/11/2020
002	**USER B**	ROLE_R	Used	2	12/05/2021
002	**USER B**	ROLE_S	Used	2	12/05/2021
002	**USER B**	ROLE_T	Used	2	12/05/2021
002	**USER B**	ROLE_U	Used	2	12/05/2021
002	**USER B**	ROLE_V	Used	2	04/06/2021
002	**USER B**	ROLE_W	Used	2	04/06/2021
002	**USER B**	ROLE_X	Used	2	04/06/2021
002	**USER B**	ROLE_Y	Used	2	04/06/2021

Figura 4.3 Tabella finale risultato dell'incrocio dei dati

4.2 Classificazione delle utenze in macroaree

Giunti a questo punto abbiamo utilizzato i dati a disposizione per poter dividere gli utenti in delle macroaree di appartenenza.

Prima di tutto utilizzando le informazioni presenti nel report HR (Job family, position title, job area and job function) abbiamo classificato gli utenti in una prima bozza di job role. Una volta divisi, abbiamo analizzato la compatibilità tra gli utenti della stessa area per capire se effettivamente le loro azioni a sistema rispecchiassero il loro ruolo effettivo.

Per fare ciò abbiamo utilizzato i dati estratti precedentemente dal transato e profilato gli utenti in base ai ruoli da loro effettivamente usati.

Per prendere visione della situazione a sistema è stato sviluppato un algoritmo che confrontasse utente per utente e creasse una matrice dove nell'incrocio tra gli utenti si trova la percentuale di compatibilità, che è data da:

$$p = 2 \times \frac{ruoli\ in\ comune\ tra\ gli\ utenti}{R_a + R_b} \times 100 \tag{4.1}$$

con p percentuale di compatibilità tra gli utenti A e B, R_a numero di ruoli dell'utente A e R_b numero di ruoli dell'utente B.

Il risultato atteso era quindi che utenti con lo stesso job role avessero un'alta compatibilità tra di loro mentre ne avessero una bassa con utenti di un job role differente. Una prima matrice è stata sviluppata per gli utenti dell'intera area Finance & Controlling, circa 300 utenze, per le quali sono stati definiti inizialmente 30 job roles. Gli utenti sono organizzati nelle righe e nelle colonne in modo che utenti che hanno lo stesso job role siano vicini tra loro, in questo modo il risultato atteso era quindi di una matrice simmetrica e

diagonale a blocchi, avendo le stesse entrate per righe e per colonne. I blocchi si intendono come zone con alta compatibilità, essendo infatti il risultato del calcolo della compatibilità tra utenti con lo stesso job role.

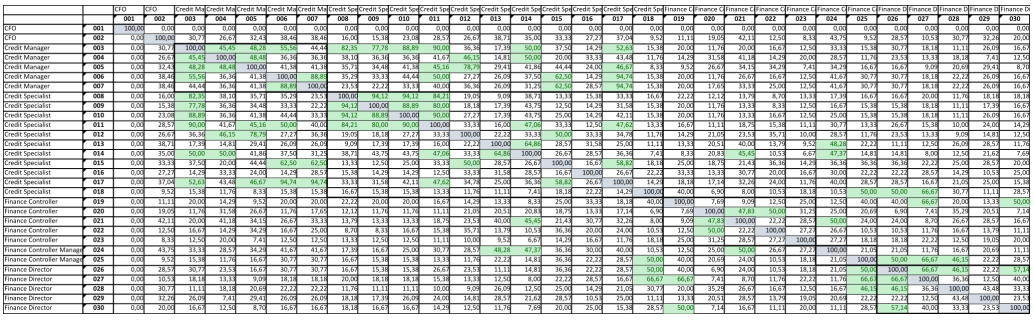


Figura 4.4 Estratto della matrice di compatibilità degli utenti

Nella figura 4.4 è presente un estratto della matrice in questione, di dimensione reale 300 x 300, nella quale i quadrati attorno alla diagonale sono evidenziati con un bordo più spesso, per mettere in luce le aree nelle quali ci si aspetta di trovare un'alta compatibilità tra utenti, evidenziata dalle celle in verde. Come in parte si evince dall'immagine il risultato ottenuto ha deluso le aspettative quindi per la maggior parte degli utenti è stato necessario condurre ulteriori analisi.

4.3 Riallocazione e controlli ulteriori

Dopo l'analisi di compatibilità, gli utenti con una bassa compatibilità tra gli altri utenti dello stesso job role sono stati:

A Riallocati, nel caso in cui la loro compatibilità fosse più alta con altri utenti di un job role già definito, in tale job role;

B Investigati ulteriormente e definito e assegnato un nuovo job role ad hoc oppure rivisto e aggiustato il contenuto del job role. Per fare ciò è stato utilizzato:

- i dati del transato presenti a sistema per identificare le transazioni eseguite;

- dal report di SuccessFactors[2] Job family, position title, job area e job function sono state usate per identificare il job role;
- dal report di SuccessFactors Legal entity, org layer e group management sono state utilizzate per definire la localizzazione dell'utente.

USER ID	Employee Status	Last Name	First Name	Position Title	Legal Entity	Group Management	Org Layer	Country/ Region	Job Area	Job Function	Job Family
000001	Active	LastName001	Name001	Financial Coordinator	AA01	XXXX	Local	Peru	XX-jobArea	SF-FI-Finance	SF-FI-PA-Financial Planning & Analysis
000002	Active	LastName002	Name002	XXXX	AB01	XXXY	Global	Italy	XX-jobArea	SF-FI-Finance	SF-FI-PA-Financial Planning & Analysis
000003	Active	LastName003	Name003	XXXY	AC01	XXXZ	Global	United States	XX-jobArea	SF-FI-Finance	SF-FI-PA-Financial Planning & Analysis
000004	Active	LastName004	Name004	Supplier Account Manager	AD02	XXYZ	Local	France	XX-jobArea	SF-FI-Finance	SF-FI-AC-Accounting
000005	Active	LastName005	Name005	Financial Analyst	BB11	XXWZ	Local	China	XX-jobArea	SF-FI-Finance	SF-FI-PA-Financial Planning & Analysis
000006	Active	LastName006	Name006	Controlling Manager	CD20	XXWY	Local	Brazil	XX-jobArea	SF-FI-Finance	SF-FI-AC-Accounting

Figura 4.5 Esempio di dati presenti nel report HR

Inoltre, visto che talvolta i dati presenti in SuccessFactors risultavano inconsistenti, ci siamo aiutati con l'analisi usando la sua position title presente nell'organigramma aziendale che è stato utilizzato anche per meglio investigare alcuni utenti: conoscendo infatti il team di lavoro di un utente è utile a posizionarlo all'interno di un job role.

Un altro strumento utile di controllo sono state alcune tabelle specifiche:

- CDHDR: tabella che registra la modifica dell'header dei documenti (La parte del documento che contiene informazioni valide per l'intero documento, e.g. data e numero del documento. Contiene inoltre informazioni di controllo come il tipo di documento);
- BKPF: tabella che contiene l'header per i documenti contabili che consiste in *Company Code*, *Document No* e *Fiscal Year*;
- MSEG: tabella che viene usate per archiviare dati di segmento di documenti relativi al materiale;
- VBAK: tabella che contiene dati relativi a documenti di vendita.

[2]SuccessFactors® è il software messo a disposizione da SAP per la gestione delle risorse umane

4.4 Creazione di specifici job roles ad hoc per gli utenti

Figura 4.6 Principali driver per la classificazione degli utenti

I nuovi job role creati sono stati strutturati in modo da avere una lista di ruoli in comune a tutti gli utenti con quel job role (ruoli kernel) ed eventualmente alcuni ruoli addizionali che variano da country a country in base alle necessità degli utenti di quelle country (ruoli delta). Per determinare in quale delle due categorie un ruolo dovesse ricadere sono stati utilizzati i seguenti criteri:

- **Ruolo kernel**: un ruolo si definisce kernel se è assegnato ad ogni utente oppure è un ruolo in solo "display" assegnato alla maggior parte degli utenti di un job role;
- **Ruolo delta**: un ruolo si identifica come delta se è stato utilizzato un numero considerevole di volte dall'utente, è stato usato recentemente ed è ulteriormente verificato ispezionando le specifiche tabelle transazionali sopra descritte per verificare l'uso che un utente ne fa. Infatti, se certe operazioni che vengono svolte tramite l'utilizzo di un ruolo possono essere svolte mediante l'utilizzo di un altro ruolo già presente si identifica quindi una ridondanza che va mitigata.

I criteri usati per l'identificazione di un ruolo delta sono stati, nello specifico quelli in figura 4.7

		ULTIMO UTILIZZO						
		<2019	12/2019	<=05/2020	<12/2020	12/2020	>01/2021	>05/2021
NUMERO DI ESECUZIONI	>100	RIMUOVERE	OK	RICHIEDERE FEEDBACK	OK	OK	OK	OK
	<100	RIMUOVERE	OK	RICHIEDERE FEEDBACK	RICHIEDERE FEEDBACK	OK	OK	OK
	<50	RIMUOVERE	OK	RIMUOVERE	RICHIEDERE FEEDBACK	OK	OK	OK
	<20	RIMUOVERE	OK	RIMUOVERE	RICHIEDERE FEEDBACK	OK	OK	OK
	<10	RIMUOVERE	OK	RIMUOVERE	RICHIEDERE FEEDBACK	OK	OK	OK
	<5	RIMUOVERE	OK	RIMUOVERE	RICHIEDERE FEEDBACK	OK	RICHIEDERE FEEDBACK	OK

Figura 4.7 Criteri di identificazione e ispezione per un ruolo delta utilizzati

Per ogni job role ci possono essere quindi due tipi di profilo assegnati ad un utente:

- Profilo contenente solo ruoli kernel;
- Profilo contenente sia ruoli kerneli che ruoli delta.

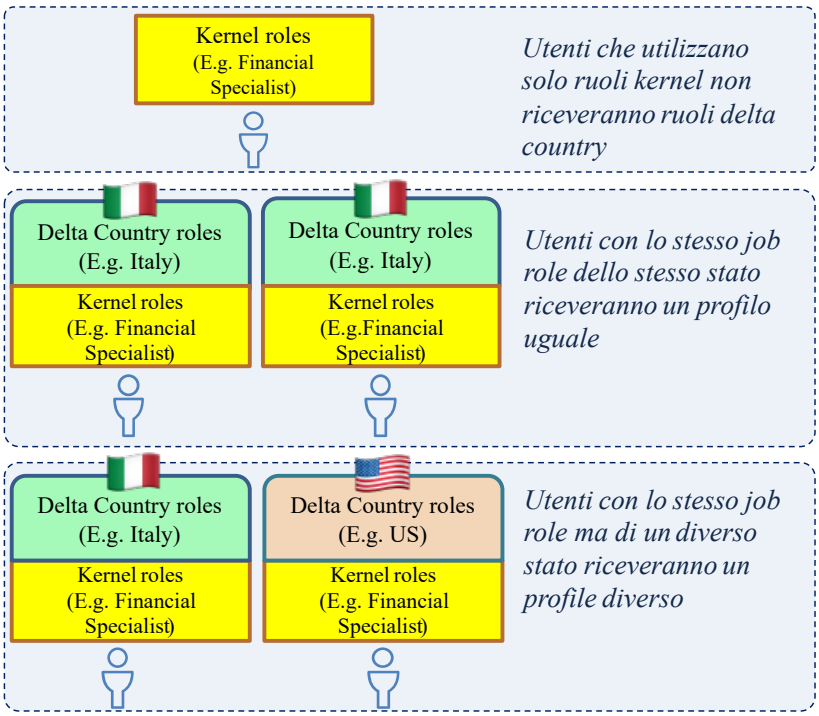


Figura 4.8 Struttura dei profili adottata

Un esempio della struttura del job role di “Financial Commercial Director”, nel quale ogni utente riceve un profilo diverso:

Financial Commercial Director

Roles Classification after analysis

KERNEL roles
ROLE_1
ROLE_2
ROLE_3
ROLE_4
ROLE_5
ROLE_6
ROLE_7
ROLE_8
ROLE_9
ROLE_10
ROLE_11
ROLE_12
ROLE_13

IT roles
ROLE_14
ROLE_15
ROLE_16
ROLE_17
ROLE_18
ROLE_19
ROLE_20
ROLE_21
ROLE_22
ROLE_23
ROLE_24

US roles
ROLE_25

AU roles
ROLE_26

Roles Attribuition to users based on their actions and countries

User	Country
User 1	IT
User 2	IT
User 2	US
User3	AU

User 1 roles: KERNEL + IT10
ROLE_1:IT
ROLE_2:IT
ROLE_3:IT
ROLE_4:IT
ROLE_5:IT
ROLE_6:IT
ROLE_7:IT
ROLE_8:IT
ROLE_9:IT
ROLE_10:IT
ROLE_11:IT
ROLE_12:IT
ROLE_13:IT
ROLE_14:IT
ROLE_15:IT
ROLE_16:IT
ROLE_17:IT
ROLE_18:IT
ROLE_19:IT
ROLE_20:IT
ROLE_21:IT
ROLE_22:IT
ROLE_23:IT
ROLE_24:IT

User 2 roles: KERNEL
ROLE_1:IT
ROLE_2:IT
ROLE_3:IT
ROLE_4:IT
ROLE_5:IT
ROLE_6:IT
ROLE_7:IT
ROLE_8:IT
ROLE_9:IT
ROLE_10:IT
ROLE_11:IT
ROLE_12:IT
ROLE_13:IT

User 3 roles: KERNEL + US
ROLE_1:US
ROLE_2:US
ROLE_3:US
ROLE_4:US
ROLE_5:US
ROLE_6:US
ROLE_7:US
ROLE_8:US
ROLE_9:US
ROLE_10:US
ROLE_11:US
ROLE_12:US
ROLE_13:US
ROLE_25:US

User 4 roles: KERNEL + AU
ROLE_1:AU
ROLE_2:AU
ROLE_3:AU
ROLE_4:AU
ROLE_5:AU
ROLE_6:AU
ROLE_7:AU
ROLE_8:AU
ROLE_9:AU
ROLE_10:AU
ROLE_11:AU
ROLE_12:AU
ROLE_13:AU
ROLE_26:AU

Figura 4.9 Esempio di job role

5 | Validazione della soluzione proposta

Essendo il go live di questo progetto previsto per maggio 2022, non vi è ancora visibilità della bontà effettiva dei job role creati, poiché una risk analysis può essere lanciata solo una volta creati ed assegnati i job role a sistema.

Essendo però stati costruiti con estrema attenzione e meticolosità, prestando attenzione anche ai minimi dettagli, gli eventuali rischi che si presenteranno non dovrebbero essere troppo rilevanti ed eventualmente saranno mitigati.

Un primo dato confortante però della bontà della soluzione, è di come si è riuscito ad effettuare una buona clusterizzazione degli utenti nelle varie aree, visibile in figura 5.1, nella quale le celle evidenziate in verde mostrano quando il numero totali di profili è inferiore al numero totale di utenti per quel job role.

In tabella 5.1 è riassunto il dettaglio dell'assegnazione e creazione dei job role, il risultato quindi finale al quale si è raggiunto dopo la fase di analisi.

Numero totale di utenti	296
Numero di ruoli kernel	272
Numero di ruoli delta	173
Totale profili creati	217
Totale job role definiti	60

Tabella 5.1 Dettaglio dell'assegnazione e creazione dei job roles

Job Role	Number of Users	Number of Different Profiles	Job Role	Number of Users	Number of Different Profiles
Job Role 1	12	12	Job Role 31	32	17
Job Role 2	23	17	Job Role 32	5	3
Job Role 3	1	1	Job Role 33	1	1
Job Role 4	1	1	Job Role 34	2	2
Job Role 5	5	5	Job Role 35	2	1
Job Role 6	1	1	Job Role 36	1	1
Job Role 7	5	4	Job Role 37	1	1
Job Role 8	12	4	Job Role 38	2	1
Job Role 9	5	5	Job Role 39	1	1
Job Role 10	2	2	Job Role 40	2	2
Job Role 11	17	16	Job Role 41	1	1
Job Role 12	1	1	Job Role 42	2	2
Job Role 13	5	4	Job Role 43	1	1
Job Role 14	4	4	Job Role 44	1	1
Job Role 15	9	8	Job Role 45	1	1
Job Role 16	22	10	Job Role 46	1	1
Job Role 17	1	1	Job Role 47	1	1
Job Role 18	4	1	Job Role 48	2	1
Job Role 19	1	1	Job Role 49	1	1
Job Role 20	20	18	Job Role 50	8	4
Job Role 21	1	1	Job Role 51	2	2
Job Role 22	1	1	Job Role 52	2	2
Job Role 23	1	1	Job Role 53	9	8
Job Role 24	2	1	Job Role 54	13	5
Job Role 25	6	3	Job Role 55	1	1
Job Role 26	2	2	Job Role 56	1	1
Job Role 27	1	1	Job Role 57	2	2
Job Role 28	6	5	Job Role 58	2	2
Job Role 29	6	6	Job Role 59	1	1
Job Role 30	7	5	Job Role 60	11	7

Figura 5.1 Dettaglio dell'assegnazione dei job role agli utenti

Un altro dato considerevole è mostrato in figura 5.2, dalla quale si evince come da una medesima tupla di valori presenti nelle colonne con header azzurro si possano identificare più di un job role, rendendo quindi impossibile l'automazione dell'assegnazione di esso durante la fase di creazione di una nuova utenza.

Employee Category	Legal Entity	Group Management	Unit	Department	Location	Org Layer	Job Area	Job Function	Job Family	Job role assigned
Employee	LE	XXXX - Group mgmt 1	ARG-Argentina	1234-Finance	1234-City	Local	XX-Job Area 1	XX-AA-Job Function 1	XX-AA-BB-Job Family 1	Job Role 1
										Job Role 2
									XX-AA-CC-Job Family 2	Job Role 3
										Job Role 4
									XX-AA-DD-Job Family 3	Job Role 5
										Job Role 6
									XX-AA-EE-Job Family 4	Job Role 7
										Job Role 8
										Job Role 9
										Job Role 10
									XX-AA-FF-Job Family 2	Job Role 11

Figura 5.2 Dettaglio dell'assegnazione dei job role agli utenti

6 | Conclusioni

In conclusione, il lavoro svolto da me e dal mio gruppo ha riscontrato soddisfazione da parte del cliente in quanto, anche se per ora solamente su carta, i job role creati presentano un buon livello di segregazione.

Ne è un esempio l'area di Financial Planning and Analysis, per la quale precedentemente vi erano solo 3 job role e a valle della nostra analisi ne sono presenti ben 15.

Aver inoltre dimostrato ad i vertici dell'azienda come l'inserimento automatizzato di un nuovo utente nella sua area di pertinenza non sia possibile secondo le modalità attuali ha portato alla luce la necessità di riflettere internamente al cliente un nuovo schema di classificazione delle utenze che possa essere più efficiente.

Parallelamente alla segregazione si è comunque riusciti ad ottenere un buon livello di raggruppamento degli utenti sotto lo stesso job role, di modo che ora gli utenti che hanno lo stesso ruolo in azienda abbiano tale ruolo rispecchiato anche a sistema, rendendo così le utenze meglio raggruppate e meglio distinguibili avendo eliminato ruoli non più necessari e definendo così un'identità più chiara.

Questo è stato permesso da una lunga fase di analisi di fino iniziale, nella quale l'analisi dei dati presenti a sistema e l'incrocio di essi con la creazione delle matrici di compatibilità hanno permesso di prendere coscienza della situazione e dare un importante punto di partenza sul quale lavorare, e successivamente la fase di interviste ai responsabili di dipartimento dei vari settori, la quale ha appunto richiesto molto tempo ma ha concesso di implementare un set di ruoli e autorizzazioni che consentiranno un aggiornamento del sistema ERP consistente e durevole nel tempo.

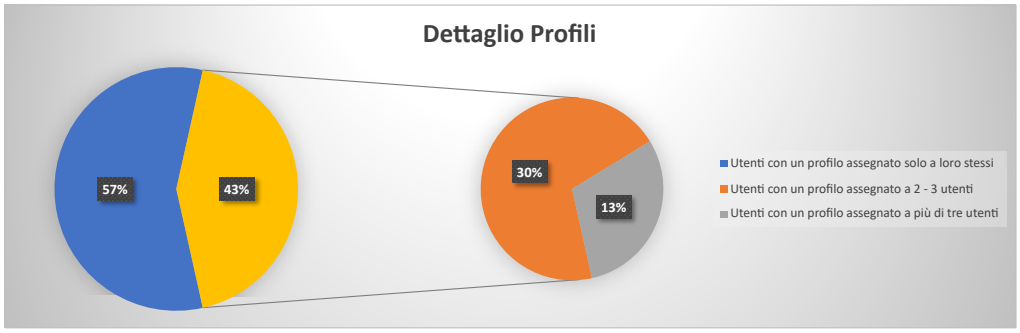


Figura 6.1 Dettaglio dell'assegnazione dei profili

Il tutto sarà affiancato da una fase di supporto post go-live che intercetterà tutte le imperfezioni e mancanze e le andrà a correggere, avvicinandosi sempre di più a un sistema sicuro al 100

Tutto il lavoro svolto consentirà all'azienda interessata di poter gestire grosse quantità di materiali, denaro e un considerevole numero di dipendenti, tre categorie tutte in aumento viste le recenti acquisizioni di altre compagnie del settore food & beverage che stanno portando l'azienda sempre più verso la leadership del suo settore nel mercato mondiale.

Bibliografia

[1] AGLEA-s.r.l., "Segregation of duties in sap." Available at :https://www.aglea.com/segregation-of-duties-in-sap.

[2] D. Walkowski, "What is the cia triad?," Jul 2019. Available at :https://www.f5.com/labs/articles/education/what-is-the-cia-triad.

[3] D. Walkowski, "What is the principle of least privilege and why is it important?," Dec 2020. Available at: https://www.f5.com/labs/articles/education/what-is-the-principle-of-least-privilege-and-why-is-it-important.

[4] "Owasp top ten." Available at: https://owasp.org/www-project-top-ten/.

[5] "The confidentiality integrity availability cia triad." Available at: https://www.researchgate.net/figure/The-Confidentiality-Integrity-Availability-CIA-triad_fig1_346192126.

[6] "Understanding segregation of duties (sod) in sap grc." Available at: https://www.secure-24.com/blog/understanding-segregation-of-duties-sod-in-sap-grc/.

[7] "What we can learn from the capital one hack," Aug 2019. Available at: https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/.

[8] R. McLean, "A hacker gained access to 100 million capital one credit card applications and accounts | cnn business," Jul 2019. Available at: https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html.

[9] G. Guthrie and M. Huffman, "Cybersecurity news," Mar 2022. Available at: ttps://www.consumeraffairs.com/news/nearly-235-million-accounts-on-instagram-tiktok-and-youtube-exposed-in-data-breach-082020.html.

[10] A. Spadafora, "Major data breach exposes database of 200 million users," Mar 2020. Available at: https://www.techradar.com/news/major-data-breach-exposes-database-of-200-million-users.

[11] J. Jason, "Hundreds of millions of facebook user records were exposed on amazon cloud server," Apr 2019. Available at: https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/.

[12] A. Spadafora, "Google cloud server left a billion people's data unsecured," Nov 2019. Available at: https://www.techradar.com/news/google-cloud-server-left-a-billion-peoples-data-unsecured.

[13] "5 major modern api data breaches (and what we can learn from them): Nordic apis," May 2020. Available at https://nordicapis.com/5-major-modern-api-data-breaches-and-what-we-can-learn-from-them/.

[14] Cyware, "A new flaw in the api of justdial found exposing personal details of reviewers: Cyware hacker news." Available at: https://cyware.com/news/a-new-flaw-in-the-api-of-justdial-found-exposing-personal-details-of-reviewers-c1bdfca3.

[15] SAP, "What is erp?," Feb 2022. Available at: https://insights.sap.com/what-is-erp/.

[16] Wikipedia, "Enterprise resource planning," Mar 2022. Available at: https://en.wikipedia.org/wiki/Enterprise_resource_planning.

[17] "Profitability and cost management release 11.1.2.4.120 administrator's guide." Available at: https://docs.oracle.com/cd/E57185_01/OHPCA/apcs01.html.

[18] Wikipedia, "Enterprise appliance transaction module," Oct 2021. Available at: https://en.wikipedia.org/wiki/Enterprise_appliance_transaction_module.

[19] Aglea-s.r.l., "Sap grc governance risk and compliance." Available at: https://www.aglea.com/sap-grc.

[20] Wikipedia, "Lightweight directory access protocol," Dec 2020. Available at https://it.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol.