Politecnico di Torino

Collegio di Ingegneria Gestionale

Corso di laurea magistrale in Ingegneria Gestionale

Tesi di Laurea di II Livello

IL RUOLO DELL'IT AUDIT – UN PROGETTO DI REVISIONE DEI SISTEMI INFORMATIVI IN UN'IMPRESA MEDIO PICCOLA TORINESE

Relatore:
Prof. Luigi Buzzacchi

Candidato:
Alberto Ferraro

Anno Accademico 2019/2020

Indice

Abstract

Il seguente lavoro è scritto in seguito ad un tirocinio svolto presso una società di consulenza. Nella prima parte dell'elaborato ho descritto quale sia il ruolo di questa figura all'interno dell'azienda, nella seconda parte ho effettuato una breve introduzione dell'azienda presso la quale ho svolto lo stage ed in seguito ho presentato il progetto di IT audit che ho seguito personalmente, assieme ad alcuni colleghi, volto alla revisione dei sistemi informativi contabili di un'impresa medio – piccola torinese, evidenziandone i passaggi principali e le criticità affrontate.

Capitolo 1

1.1 Che cos'è il processo di revisione contabile?

La revisione contabile consiste in una serie di attività e procedimenti campionari svolti da un soggetto, il revisore legale, al fine di verificare la veridicità dei dati contenuti in un bilancio di esercizio o in un bilancio consolidato (Wikipedia, s.d.)[1].

Il bilancio d'esercizio è un insieme di documenti contabili che ogni impresa deve redigere periodicamente alla fine di ogni esercizio amministrativo. Affinché questo documento possa rappresentare efficacemente l'andamento patrimoniale, finanziario ed economico dell'azienda deve essere redatto rispettando i principi fondamentali, contenuti nell'art.2423 del Codice Civile, elencati di seguito (EconomiaAziendale, s.d.)[2]:

- chiarezza: il bilancio deve essere redatto in modo che le informazioni in esso contenute siano chiare, cioè di facile lettura per tutti gli stakeholders, e complete;
- verità: il bilancio deve rappresentare in modo veritiero la situazione dell'azienda, ovvero in modo imparziale e senza distorsioni, manipolazioni o occultamenti;
- correttezza: il bilancio deve essere redatto applicando correttamente i principi contabili elencati nell' art.2423-bis del Codice Civile.

Lo scopo generale del bilancio è quello di fornire informazioni sulla posizione finanziaria, sui risultati operativi, e sui flussi di cassa di un'organizzazione. Queste informazioni sono utilizzate da molti attori: sia interni, ad esempio i manager che decidono quali direzioni di business intraprendere; sia esterni, come i potenziali investitori che utilizzano i documenti di bilancio per comprendere al meglio le potenzialità dell'impresa e i rischi associati all'acquisto di partecipazioni di una

[1] Wikipedia, *Revisione Contabile:* https://it.wikipedia.org/wiki/Revisione_contabile
[2] EconomiaAziednale.net, *Principi di redazione del bilancio d'esercizio:* https://www.economiaziendale.net/bilancio/principi_redazione_bilancio_esercizio.htm

determinata azienda. Pertanto, è fondamentale che le informazioni contenute nel bilancio rappresentino in maniera affidabile la posizione finanziaria e non contengano errori significativi, dovuti a frodi o eventi non intenzionali. In seguito a questa necessità da parte degli stakeholder, sempre più rilevante nel corso degli anni, le aziende si sono affidate a figure esterne per ottenere una valutazione della correttezza dei dati iscritti a bilancio e colmare la grande asimmetria informativa, questo procedimento prende il nome di "revisione contabile".

È da precisare che la certificazione di bilancio non sta ad indicare un buono stato di salute finanziaria dell'azienda revisionata, ma indica che il bilancio d'esercizio non è fonte di informazioni errate.

In Italia, a partire dal 1975, anno in cui col d.p.r. n. 136[3] è stato istituito l'obbligo della certificazione per le società per azioni quotate in borsa, numerose leggi hanno progressivamente esteso quest' obbligo a categorie sempre più ampie di imprese e, praticamente, quasi tutte le norme che assegnano contributi o sovvenzioni statali prevedono anche la revisione dei bilanci. Tuttavia, negli ultimi anni, sono sempre di più le imprese, anche di piccole o medie dimensioni, che sottopongono a revisione volontaria il proprio bilancio e questo trend è destinato a crescere in futuro (Cassandrelli, 2006)[4].

[3] Attuazione della delega di cui all'articolo 2, lettera a, della legge 7 giugno 1974, n. 216 concernente il controllo contabile e la certificazione dei bilanci delle società per azioni quotate in borsa

[4] S. Cassandrelli, *PICCOLE E MEDIE IMPRESE: PERCHE LA REVISIONE CONTABILE?,* 2006

1.2 Introduzione dei sistemi informativi contabili

In tempi passati la rendicontazione finanziaria e contabile delle imprese era tenuta manualmente, tuttavia intorno ai primi anni '70, per assicurare una maggior correttezza e rapidità di calcolo, le aziende cominciarono ad utilizzare i primi sistemi informativi che le permettevano di registrare ed elaborare informazioni abbastanza semplici, come ad esempio le paghe dei dipendenti. A mano a mano che la complessità dei processi aziendali è aumentata i sistemi informativi si sono evoluti e sviluppati ed il sistema contabile ha subito una trasformazione radicale, da semplice contenitore ed elaboratore di dati finanziari a fonte informativa primaria dell'azienda e mezzo di supporto fondamentale per le decisioni dei dirigenti (Pampolini, 2017)[5].

Il sistema informativo contabile può essere definito come un insieme sistemico di dati elementari, elaborazioni contabili e statistiche, aggregazioni e scomposizioni di dati, di informazioni varie, che offrono all'azienda, gli elementi per:

- effettuare le opportune decisioni imprenditoriali;
- essere al corrente e controllare l'attività svolta al fine di poter intervenire tempestivamente qualora ve ne sia la necessità;
- determinare il risultato economico d'esercizio e il patrimonio di funzionamento;
- documentare ai fini fiscali le dichiarazioni presentate (Presti, 2016)[6]

L'utilizzo dei sistemi informativi porta alle aziende notevoli vantaggi:

- dal punto di vista economico, poiché permetteranno all'azienda di risparmiare sul personale umano che in precedenza era occupato a svolgere determinate mansioni;

[5] K. Pampolini, *L'evoluzione della gestione informativa aziendale: benefici, criticità e supporto alle organizzazioni,* Università di Venezia, 2017
[6] C. Presti, *L'INTEGRAZIONE DEL SISTEMA INFORMATIVO - CONTABILE: EVOLUZIONE STORICA E PROSPETTIVE FUTURE,* Università di Pisa, 2016

- dal punto di vista dell'efficienza, poiché l'utilizzo di sistemi computerizzati garantisce sia la gestione di una quantità notevole di dati in un tempo estremamente più breve rispetto a quello impiegato dalla manodopera umana, sia una maggiore accuratezza.

Quindi, col tempo, i sistemi informatici hanno assunto un ruolo fondamentale per le aziende, come mezzo di immagazzinamento dei dati e come mezzo di supporto ai processi decisionali, poiché attraverso l'elaborazione di elevate quantità di dati sono in grado di consegnare ai dirigenti aziendali informazioni molto più ricche e precise. Tuttavia, vista l'importanza che hanno iniziato ad assumere nella realtà aziendale, non è possibile affidarsi unicamente alla tecnologia, poiché le applicazioni e i sistemi informatici devono essere valutati attentamente. Entra in gioco un processo che negli ultimi anni ha svolto un ruolo essenziale nel panorama aziendale: l'internal audit, ovvero: "Un'attività indipendente e obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto, in quanto finalizzato a valutare e migliorare i processi di gestione dei rischi, di controllo, e di governance"[7]. (AIIA, s.d.) Più precisamente, quando si parla di tecnologie informatiche, si fa riferimento all'audit IT, ovvero un processo di verifica sistematico e documentato, condotto da personale esperto e imparziale, che i sistemi informativi di un'azienda o organizzazione siano conformi a quanto previsto da norme, regolamenti e politiche interne (Wikipedia, s.d.)[8]. Questo comporta l'applicazione di protocolli di efficienza e sicurezza, e processi di supervisione IT. L'applicazione dei controlli è necessaria ma non sufficiente per fornire un'adeguata sicurezza. Le persone responsabili devono verificare che i controlli

[7] Definizione di IA, AIIA: https://www.aiiaweb.it/definizione-di-internal-auditing#:~:text=Definizione%20di%20Internal%20Auditing,dell'efficienza%20dell'organizzazione.
[8] *Audit Interno -IT audit o revisione dei sistemi informativi ,* Wikipedia: https://it.wikipedia.org/wiki/Audit_interno#:~:text=L'IS%20auditing%20(in%20italiano,norme%2C%20regolamenti%20o%20politiche%20interne.

siano eseguiti, che siano efficaci oppure no e, in tal caso, quali azioni possono essere intraprese per prevenire future inefficienze (Gantz, 2014)[9].

Nell'ambiente IT vi è inoltre una serie di rischi legata all'accesso da parte di individui a software, hardware e componenti dell'ambiente tecnologico inerenti all'uso di modifiche non autorizzate o imperfette ai programmi che possono introdurre errori o causare elaborazioni incomplete, questi rischi devono essere mitigati e controllati per proteggere i processi aziendali.

Dunque, il processo di revisione legale è svolto congiuntamente al processo di audit IT, poiché per verificare che il bilancio non contenga errori rilevanti, bisogna anche assicurarsi che le informazioni generate dai sistemi informativi siano affidabili e dunque che questi ultimi funzionino correttamente.

[9] Gantz, Stephen D. (2014). *The basics of IT audit: purposes, processes, and practical information*. 2014: Syngress, an imprint of Elsevier

1.3 Nuovi rischi legati ai sistemi informativi

Nel panorama moderno i sistemi informativi svolgono un ruolo fondamentale nel supporto aziendale, tuttavia espongono coloro che decidono di utilizzarli ad una serie di rischi che possono provocare enormi perdite a causa di errori nella gestiome di questi sistemi, inefficienze nei processi, minacce informatiche o comportamento fraudolento da parte del personale interno.

Il rischio IT ha molte definizioni, tutte simili tra loro, di seguito si è deciso di riportare quella proposta dall'associazione ISACA (Information Systems Audit and Control Association): "Il rischio IT è un rischio aziendale, in particolare il rischio aziendale associato all'uso, alla proprietà, all'utilizzo, al coinvolgimento, all'influenza e all'adozione dell'IT all'interno di un'azienda. Consiste in eventi e condizioni legati all'IT che potrebbero potenzialmente avere un impatto sull'azienda. Può verificarsi con frequenza e incidenza incerte e crea problemi nel raggiungimento di obiettivi e traguardi strategici (ISACA, 2009)[10]"

Dunque, come si evince dalla definizione, anche un utilizzo marginale da parte di un'azienda di un sistema informativo la espone ad un rischio, che può generare ingenti perdite, malfunzionamenti o fuga di dati all'esterno dell'organizzazione, se trascurato. È quindi fondamentale che il management dedichi molta attenzione alla gestione dei sistemi informativi poiché anche un piccolo errore potrebbe portare a gravi conseguenze economiche e reputazionali.

I rischi che una determinata organizzazione deve affrontare dipenderanno dalla natura delle attività e delle operazioni dell'organizzazione, dal settore in cui l'organizzazione opera, la configurazione dei sistemi informativi dell'organizzazione e vari altri fattori interni ed esterni. Esistono, tuttavia, alcuni tipi di rischi IT che tendono ad essere comuni tra organizzazioni e settori:

[10] *The Risk IT Framework,* ISACA, USA, 2009

- Rischio di selezione: selezione di una soluzione IT non allineata all'obiettivo può precludere l'esecuzione della strategia dell'azienda;
- Rischio di sviluppo / acquisizione e implementazione: il sistema informativo in fase di sviluppo/acquisizione e implementazione può causare ritardi imprevisti, eccessivi costi o persino l'abbandono del progetto;
- Rischio di disponibilità: l'indisponibilità del sistema quando necessario può causare ritardi nel processo decisionale, interruzioni dell'attività, e perdita di ricavi;
- Rischio hardware/software: il mancato funzionamento corretto dell'hardware/software può causare interruzioni dell'attività, distruzione dei dati e costi di riparazione o sostituzione;
- Rischio di accesso: poterebbero verificarsi accessi al sistema non autorizzati con conseguente furto o distruzione dei dati;
- Affidabilità del sistema e rischio dell'integrità delle informazioni: errori sistematici o incoerenze nell'elaborazione dei dati possono produrre incomplete o inesatte.
- Rischio di frode: un'errata separazione dei compiti può permettere ai dipendenti di compiere frodi.

È fondamentale che le aziende che utilizzano questo tipo di tecnologie si impegnino a proteggere l'ambiente IT e controllarlo, affinché possano ottenere le migliori performance aziendali e possano adeguarsi ai requisiti di rischio, governance e conformità.

Vista l'importanza dell'informativa e trasparenza societaria e a seguito di numerosi scandali finanziari che hanno spiazzato la fiducia degli investitori, come il caso Enron, avvenuti ne primi anni 2000, sono nate numerose normative a riguardo, ad esempio il Sarbane – Oxley Act (SOX) nel 2002, del quale la sezione 404 è particolarmente significativa per l'Information Tecnology.

1.4 Gli scandali dei primi anni 2000

All'inizio degli anni 2000, il ruolo della contabilità e della professione di revisore contabile è cambiato drasticamente, in seguito alla scoperta numerosi scandali contabili che minarono seriamente la fiducia che gli investitori riponevano nei mercati finanziari e nelle società di revisione (Valsania, 2013)[11]. Negli USA i più importanti furono i casi Enron, WorldCom, Adelphia, Tyco. Negli anni precedenti queste società stavano crescendo molto ed erano considerate solidissime, tuttavia, in poco tempo, il valore delle azioni crollò e ciò fece perdere miliardi di dollari agli investitori, oltre alle decine di migliaia di dipendenti che persero il posto di lavoro. Questo accadde perché si scoprì che i bilanci non rappresentavano una situazione economico finanziaria veritiera, ma la contabilità era stata alterata per anni dai dirigenti.

Alcune tra queste aziende si erano affidate allo società di revisione Arthur Andersen, facente parte delle Big Five, che anch'essa fu ritenuta responsabile delle irregolarità contabili e nell'agosto del 2002 smise di operare in seguito all' accusa di ostruzionismo alla giustizia per aver distrutto documenti relativi alla sua revisione del bilancio di Enron.

Il caso Enron rappresenta perfettamente la manifestazione di questi comportamenti fraudolenti e fu il primo ad essere scoperto che poi diede vita a innumerevoli processi ai danni di altre compagnie, che portarono all'emanazione di nuove leggi mirate a tutelare maggiormente gli investitori e recuperare la fiducia dei mercati internazionali la prima delle quali è la Sarbane – Oxley (SOX) del 2002.

1.4.1 Il caso Enron

Enron fu una delle più grandi multinazionali degli Stati Uniti operante nel campo dell'energia, che tra il 1996 e il 2000 ha registrato e incrementato le vendite da 13,3 miliardi a 100,8 miliardi di dollari e nello stesso periodo ha più che raddoppiato le sue

[11]M. Valasina, *La madre di tutte le truffe contabili: lo scandalo Enron 12 anni dopo*, Il sole 24 ore

vendite dichiarate. Prima di dichiarare all'improvviso bancarotta, Enron impiegava circa 19.000 dipendenti.

Il caso Enron costituisce uno degli esempi emblematici di fallimento dei processi di revisione contabile. La società di revisione *Arthur Andersen*, a cui era stata affidata la verifica dei bilanci, aveva di fatto coperto il sistema fraudolento di bilanci truccati messo in atto da Enron allo scopo di evadere la tassazione e generare profitti gonfiati, ignorando perdite per oltre 1 miliardo di dollari. I bilanci societari sono stati alterati in maniera sostanziale soprattutto grazie ad "interventi" sulle controllate estere, utilizzate per occultare i relativi debiti societari.

Il prezzo delle azioni di Enron, inizialmente considerate solidissime, passò dalla quotazione massima di 90,36 $ raggiunta a fine dicembre del 2000 a 0,26 $ nel giro di pochi mesi.

Il Presidente della Commissione dell'Energia e del Commercio della Camera dei Deputati USA diede l'avvio a un'investigazione sul caso in oggetto, ed Enron finì sotto inchiesta con incluse le sue 14 controllate.

Gli illeciti adoperati da Enron furono:

a) Operazioni simulate di vendita, che sono transazioni in cui non c'è nessuna contropartita effettiva (sembra che Enron abbia avuto "trading con sé stesso"), gonfiando i suoi ricavi e il valore dell'Attivo, senza alcun beneficio economico tangibile;

b) Contabilità Mark-to-Market, dove Enron ha registrato alcune transazioni di energia ai valori di mercato corrente creando un falso contabile;

c) Registrazione delle Entrate, dove Enron contabilizzava le entrate ancora prima che la fornitura di energia venisse realmente utilizzata.

La gravità dello scandalo e il conseguente crollo della fiducia degli investitori furono alla base della riforma epocale operata dal governo federale statunitense in materia societaria. Seguirono vari provvedimenti legislativi che portarono ad una progressiva omogeneizzazione della normativa di settore.

1.4 Il Sarbanes – Oxley Act

Il Sarbanes – Oxley Act, emanato il 30 luglio 2002, è la prima legge dagli USA in risposta agli scandali finanziari sopra citati, che, con lo scopo di ristabilire la fiducia degli investitori nel settore societario e dei mercati internazionali, fissa nuovi codici di autoregolamentazione e obblighi di legge e rivoluziona il concetto di trasparenza nell'informativa contabile. Secondo il presidente americano Bush, si è trattato "della più profonda riforma della gestione d'impresa dai tempi di Roosvelt" e dai Securities Acts del 1933 e 1934 (Fortunato, 2004)[12].

Le principali introduzioni volte ad aumentare della fiducia degli investitori e la protezione degli azionisti contro possibili frodi sono:

- obbligo di certificare tutte le informazioni finanziarie;
- la trasparenza delle scritture contabili;
- la predisposizione di controlli interni per la regolarità e la tracciabilità delle informazioni finanziarie;
- la responsabilità personale e oggettiva del CEO (Chief Executive Officer) e del CFO (Chief Financial Officer) che si rendono colpevoli di non fornire una rappresentazione veritiera e corretta del bilancio;
- l'aumento delle pene per il falso in bilancio e altri illeciti fiscali;
- la costituzione del Public Company Accounting Oversight Board, ossia un consiglio di vigilanza sui bilanci delle aziende quotate.

La SOX è composta da diverse sezioni, ognuna delle quali stabilisce diversi requisiti per la gestione aziendale. Le sezioni principali della normativa sono: la 302, la 404 e la 802, che sottolineano, rispettivamente, la responsabilità personale dei dirigenti dell'azienda, la necessità di mantenere un sistema di controllo interno e di archiviare tutta la corrispondenza.

[12] Fortunato S., Il provvedimento del Public Company Accounting Oversight Board, Rivista dei Dottori Commercialisti, 2004

Nella sezione 302 è sancito che il CEO e il CFO sono direttamente responsabili per l'accuratezza, la documentazione e la presentazione di tutte le relazioni finanziarie e, in particolare, per ogni relazione annuale o trimestrale presentata affermano che:

- il firmatario ha esaminato la relazione;
- il rapporto non contiene dichiarazioni false o fuorvianti;
- I rendiconti finanziari e le informazioni correlate presentano in modo equo le condizioni finanziarie e i risultati in tutti gli aspetti rilevanti;
- I funzionari firmatari sono responsabili per i controlli interni e hanno valutato tali controlli interni nei novanta giorni precedenti e hanno riferito sui risultati ottenuti;
- Un elenco di tutte le carenze nei controlli interni e informazioni su eventuali frodi che coinvolgono dipendenti coinvolti in attività interne;
- Eventuali cambiamenti significativi nelle procedure interne controlli o fattori correlati che potrebbero avere un impatto negativo sui controlli interni[13].

Inoltre, in questa sezione, è specificato che le organizzazioni non possono tentare di evitare questi requisiti reincorporando le proprie attività o trasferendo le proprie attività al di fuori degli Stati Uniti.

La sezione 404 è la più complicata, la più contestata e la più costosa da implementare di tutte le sezioni contenute nell' Sarbanes - Oxley Act. Quest'ultima richiede al management e al revisore esterno di riferire sull'adeguatezza del controllo interno della società sull'informativa finanziaria.

Il management deve:

- Accettare la responsabilità circa l'efficacia del controllo interno sull'informativa finanziaria;

[13] https://www.sarbanes-oxley-101.com/SOX-302.htm

- Comprendere il flusso delle transazioni, compresi gli aspetti IT, in modo sufficientemente dettagliato per identificare i punti in cui potrebbe sorgere un errore;
- Valutare l'efficacia dell'del controllo interno sull'informativa finanziaria applicando un criterio di controllo appropriato (ad esempio COSO);
- Eseguire una valutazione del rischio di frode;
- Valutare i controlli progettati per prevenire o rilevare frodi;
- Valutare i controlli sul processo di rendicontazione finanziaria di fine periodo.

Alla sezione 404 della normativa sono state rivolte spesso critiche, prevalentemente a difesa delle aziende con un fatturato relativamente basso. Infatti, il costo di conformità con SOX 404 incide in modo sproporzionato sulle piccole imprese, in quanto comporta un costo fisso significativo per il completamento della valutazione. Ad esempio, nel 2004 le società statunitensi con ricavi superiori a $ 5 miliardi hanno speso lo 0,06% delle entrate per la conformità SOX, mentre le aziende con ricavi inferiori a $ 100 milioni hanno speso il 2,55% (SEC, 2006)[14].

La sezione 802 del Sarbanes - Oxley Act impone una pena detentiva fino a 20 anni per alterazione, distruzione, mutilazione, occultamento, falsificazione di documenti, documenti o oggetti tangibili con l'intento di ostacolare, impedire o influenzare un'indagine legale. Impone inoltre incarcerazione fino a 10 anni a qualsiasi contabile, revisore contabile o altro che violi consapevolmente e intenzionalmente i requisiti di manutenzione di tutti i documenti di revisione o revisione per un periodo di 5 anni.

La sezione 906 impone di redigere una certificazione in cui è richiesto al CEO e ai CFO di firmare e certificare la relazione periodica contenente i rendiconti finanziari. La suddetta dichiarazione esecutiva deve affermare che la relazione è conforme ai requisiti di reporting della SEC e rappresentare correttamente la condizione

[14] SEC advisory committee on smaller public companies, *Final report of the advisory commitee on smaller public companies to the U.S. securities and exchange commission, 2006, Washington DC*

finanziaria dell'azienda e i risultati delle sue operazioni. Il mancato rispetto di questo requisito comporta multe fino a 5 milioni di dollari e può essere imposta la reclusione fino a 20 anni per non conformità consapevole o intenzionale. (SOX Section 906: Corporate Responsibility for Financial Reports, 2005)[15]

Entrambe le serie di requisiti di certificazione di cui alle sezioni 302 e 906 sono necessarie, anche se si sovrappongono in modo significativo. Tuttavia, una certificazione fraudolenta della sezione 302 è soggetta all'applicazione civile da parte della Commissione, mentre una certificazione fraudolenta della sezione 906 comporta sanzioni penali applicabili dal Dipartimento di giustizia. (Protiviti, 2007) [16].

La normativa SOX si applica a tutte le entità che hanno una classe di titoli registrata ai sensi della Sezione 12 dello Exchange Act, o che sono tenute a presentare rapporti ai sensi della Sezione 15 (d) del Securities Exchange Act del 1934 (Lander, 2004)[17].

Nello specifico, la SOX si applica a tutte le società americane e alle società di diritto estero quotate al NYSE (New York Stock Exchange).

La Public Company Accounting Oversight Board (PCAOB) è una società senza scopo di lucro, la quale verifica che principi contabili SOX siano correttamente applicati e supervisiona gli audit delle società pubbliche e di altri emittenti al fine di proteggere gli interessi degli investitori. In precedenza, la professione era autoregolata. (About the PCAOB, s.d.)[18] Tutte le norme e gli standard PCAOB devono essere approvati dalla Securities and Exchange Commission (SEC) degli Stati Uniti. Attraverso la creazione del PCAOB, il Sarbanes - Oxley Act impone che i revisori delle società pubbliche statunitensi siano soggetti per la prima volta ad una supervisione esterna e indipendente.

[15] *SOX Section 906: Corporate Responsibility for Financial Reports*, Sarbanes Oxley, https://www.sarbanes-oxley-101.com/SOX-906.htm
[16] GUIDE TO THE SARBANES-OXLEY ACT: Internal Control Reporting Requirements (Fourth Edition), protiviti
[17] Guy P. Lander, *What is Sarbanes – Oxley?, McGraw – Hill, 2004, USA.*
[18] PCAOB; Washington, DC: Public Company Accounting Oversight Board, http://pcaobus.org/About/Pages/default.aspx

Capitolo 2

Intorno alla metà degli anni 2000 iniziò ad aumentare l'importanza affidata ai controlli interni delle aziende e alla verifica di questi controlli da parte di personale esterno a queste ultime; sia da parte delle società quotate nel mercato americano sottoposte alla normativa SOX che impone la revisione dei controlli interni e il rispetto degli standard dettati dal PCAOB, sia da parte delle altre società non obbligate per legge.

Un sistema di controllo interno è definito da un insieme di meccanismi, regole e procedure che un'azienda implementa per garantire l'integrità delle informazioni finanziarie e contabili, per promuovere la responsabilità e per prevenire le frodi. Tuttavia, col tempo la materia ha avuto un'evoluzione tale per cui la definizione dei controlli non si basa solo più su questioni contabili e finanziarie, ma si estende a quasi tutti gli aspetti aziendali. Nello specifico, data l'ampia integrazione che la funzione ICT ha con i vari processi aziendali, i controlli relativi all'IT sono diventati una parte importante nella definizione di un sistema di controllo interno. Un'unità o processo aziendale ha buoni controlli interni se:

- Produce dati accurati e affidabili;
- È conforme alle leggi e alle politiche aziendali;
- Utilizza in maniera efficiente le sue risorse,
- Prevede un'adeguata salvaguardia degli asset aziendali (Moeller, 2010)[19].

Oltre a rispettare le leggi e i regolamenti ed impedire ai dipendenti di appropriarsi dei beni aziendali o commettere frodi, i controlli interni possono aiutare a migliorare l'efficienza operativa migliorando l'accuratezza e la tempestività dell'informativa finanziaria (Kenton, 2019)[20], aiutano a raggiungere gli obiettivi e tendono a migliorare le funzioni societarie. I controlli interni sono diventati una procedura chiave per molte

[19] Robert Moeller, *IT Audit, Control, and Security*, Wiley, 2010, USA.
[20] Will Kenton, *Internal Controls,* 2019, Investopedia, https://www.investopedia.com/terms/i/internalcontrols.asp

aziende, per questo motivo è fondamentale che siano efficienti nel rilevare errori che possono essere commessi nello svolgimento delle operazioni quotidiane.

Lo scenario in cui operano gli Auditor è rapidamente evoluto negli ultimi anni e con esso sono cambiati i sistemi di controllo, sempre più integrati per garantire maggiore efficacia ed efficienza nella governance delle imprese. Anche la qualità dei sistemi di controllo è quindi diventata un vero e proprio fattore di competizione (Un punto di riferimento nel sistema di controllo integrato, s.d.).

Un buon approccio all'utilizzo di un sistema di controllo interno viene vincolato quando si ricerca la conformità alla normativa SOX. Esso non crea un ambiente totalmente privo di rischi, tuttavia il processo che le aziende seguono per migliorare il proprio sistema di controllo interno e per conformarsi al Sarbanes - Oxley Act fornisce benefici durevoli. Una corretta governance riguardo la pianificazione e il ciclo di vita degli obiettivi di controllo dovrebbe portare a reporting finanziari più accurati e tempestivi (AIEA, 2006)[21].

I processi aziendali sono diventati, con gli anni, dei meccanismi sempre più articolati, dunque implementare, gestire e valutare continuamente un sistema di controlli interno risulta essere un'operazione complessa, per questi motivi sono stati progettati dei framework di riferimento, come ad esempio il "COSO Famework" che è il più diffuso ed utilizzato.

Il COSO, che è stato indicato dalla SEC come modello a cui ispirarsi per fare in modo che la gestione dei controlli interni sia conforme alla SOX, dà anche una definizione di controllo interno: "il controllo interno è un processo, stabilito dal consiglio di amministrazione e dal management, progettato per fornire ragionevoli garanzie in merito al raggiungimento degli obiettivi nelle seguenti categorie:

- efficienza ed efficacia delle attività operative;
- affidabilità dell'informativa finanziaria;

[21] Il ruolo dell'IT nel progetto e nell'implementazione dei controlli interni per la predisposizione del reporting finanziario, AIEA, 2007, Milano

- conformità alle leggi e ai regolamenti. (U. Gelinas, 2008)"[22]

Per ottenere un adeguato sistema di controllo interno è necessario svolgere cinque operazioni:

1. **Ambiente di Controllo**: l'insieme di standard, processi e strutture che forniscono le basi per lo svolgimento del controllo interno all'interno dell'organizzazione. Il consiglio di amministrazione e l'alta dirigenza stabiliscono il tono più alto in merito all'importanza del controllo interno, compresi gli standard di condotta previsti. L'ambiente di controllo comprende l'integrità e i valori etici dell'organizzazione; i parametri che consentono al consiglio di amministrazione di esercitare le proprie responsabilità di controllo della governance; la struttura organizzativa e l'attribuzione di autorità e responsabilità; il processo per attrarre, sviluppare e trattenere individui competenti; e il rigore riguardo alle misure di performance, incentivi e premi per guidare la responsabilità. L'ambiente di controllo che ne risulta ha un impatto pervasivo sul sistema complessivo di controllo interno;
2. **Valutazione dei rischi**: processo dinamico e iterativo per identificare e valutare i rischi e le frodi che l'organizzazione può incontrare nel raggiungimento degli obiettivi. Dopo aver identificato i rischi deve implementare dei piani di monitoraggio e degli strumenti di Governance, Risk management e compliance
3. **Attività di controllo**: sono le attività che aiutano a garantire che le direttive del management volte a mitigare i rischi siano realizzate. Le attività di controllo vengono eseguite a tutti i livelli dell'organizzazione, in varie fasi all'interno dei processi aziendali e nell'ambiente tecnologico. Possono essere di natura preventiva o investigativa e possono comprendere una serie di attività manuali e automatizzate come autorizzazioni e approvazioni, verifiche delle SoD (Segregation of Duties), riconciliazioni, revisioni delle prestazioni aziendali.

[22] U. Gelinas, R. Dull,P. Wheeler, *Accounting Information Systems 8th edition, Cengage Learning, 2008, Canada*

4. **Informazioni e comunicazione**: è il processo continuo di fornitura, condivisione e acquisizione delle informazioni. Internamente sono diffuse in tutta l'organizzazione informazioni riguardo gli obiettivi del sistema di controllo interno e i risultati della valutazione dei rischi. Esternamente sono condivise le relazioni periodiche e annuali.
5. **Monitoraggio**: processo che valuta la qualità delle prestazioni del sistema di controllo interno nel tempo. Le carenze del controllo interno rilevate attraverso queste attività di monitoraggio devono essere segnalate a monte e devono essere adottate misure correttive per garantire il miglioramento continuo del sistema.

2.1 Perché effettuare un audit IT?

L'esecuzione, il supporto e la gestione di un programma di audit IT sono attività che richiedono tempo, impegno e impiego di personale, quindi è ragionevole chiedersi perché le organizzazioni intraprendano questo processo. L'audit IT fornisce informazioni che aiutano le organizzazioni a gestire i rischi, ad organizzare in maniera efficiente l'allocazione delle risorse relative all'IT ed a raggiungere gli obiettivi aziendali. I motivi per giustificare gli audit IT possono essere più vari tra le organizzazioni, ma spesso includono:

- valutazione del l'efficacia dei controlli implementati;
- verifica dell'adesione a politiche, processi e procedure interne;
- verifica della conformità alla governance IT e agli standard di controllo;
- analisi delle vulnerabilità e delle configurazioni per supportare il monitoraggio continuo;
- identificare debolezze e carenze della gestione del rischio;
- misurare le prestazioni rispetto a parametri di riferimento di qualità o accordi sul livello di servizio;

L'audit IT è anche guidato dalla necessità o dal desiderio di dimostrare la conformità a standard, regolamenti o requisiti imposti esternamente al tipo di organizzazione, settore o ambiente operativo, infatti è obbligatorio per quelle aziende che sono sottoposte alla normativa SOX, che quindi devono avere un sistema di controlli interni certificato da un revisore esterno. In questi casi il processo di audit IT è essenziale per la valutazione del sistema di controllo interno stesso e per il supporto del processo di revisione contabile, poiché verifica l'efficacia e l'adeguatezza dei controlli che l'azienda effettua sui propri sistemi informativi che trattano ed elaborano i dati e le informazioni dell'azienda. Tale processo verifica quindi, con un determinato grado di confidenza, che le informazioni relative alla

rendicontazione finanziaria elaborate dai sistemi informativi non siano affette da distorsioni.

2.2 Come si svolge il processo di Audit IT: il processo di pianificazione

La fase di pianificazione dell'audit e dei controlli è fondamentale, poiché permette di:

- individuare gli obiettivi che si intende perseguire;
- formulare una stima di risorse umane e informatiche che verranno utilizzate durante il processo di audit;
- effettuare una programmazione del lavoro e stimare una durata del processo di audit.

Una prima parte del processo di pianificazione è svolta dai revisori contabili, che effettuano un'analisi dei processi che la società revisionata utilizza per gestire il bilancio e la rendicontazione finanziaria. Attraverso questa indagine sono in grado di rilevare le "significant class of transactions" (SCOTs) ovvero le voci di bilancio che incidono maggiormente sui conti della società. Una volta rilevate le SCOTs i revisori IT sono in grado di identificare quali sono gli applicativi critici per la società che vanno a incidere su queste voci di bilancio.

Durante la fase di pianificazione il team di audit IT che deve programmare il piano di revisione dei sistemi informativi si impegna a ottenere informazioni riguardo ad aspetti fondamentali dell'organizzazione in scopo e redige dei documenti a cui potrà fare riferimento durante tutto il ciclo di audit: comprensione dell'ambiente IT e pianificazione delle attività.

Il primo è un documento nel quale è descritto l'ambiente IT, "lo scopo del lavoro di rilevazione del sistema IT aziendale è quello di fornire una review ad alto livello del sistema informativo dell'Azienda, evidenziando i cambiamenti avvenuti e in corso di attuazione. Le informazioni generalmente riguarderanno le seguenti aree:

• Descrizione generale dei Sistemi Informativi

• Organizzazione della Direzione IT

• Software applicativo

• Modalità di esecuzione delle modifiche/nuovi sviluppi software

• Sicurezza logica e fisica

• Business Continuity e Disaster Recovery Plan

• Conformità legale

• Progetti in corso di attuazione" (LaRevisioneLegale, 2012).

Il secondo documento è redatto dopo aver effettuato un primo incontro con il referente IT dell'azienda, nel quale sono pianificate le attività di audit IT. Al suo interno contiene più sezioni, che indicano:

- Mappatura degli ambienti IT dell'azienda: analisi dei sistemi operativi e dei software utilizzati, gli hardware e la loro ubicazione e infine analisi dei processi IT. Questa informazione fornisce al revisore una comprensione dei rischi connessi.
- Stima delle tempistiche dell'intervento di audit;
- Personale coinvolto nell'attività;
- Identificazione dei rischi e criticità dei sistemi IT, per capire quali dei sistemi possono essere classificati come sistemi critici, ovvero quelli il cui fallimento avrebbe un impatto grave sull'organizzazione.
- Predisposizione degli applicativi che saranno testati e dei controlli che verranno effettuati
- Stima del budget per l'intera attività di Audit.

2.2 Risk assessment

Una fase cruciale del processo di pianificazione dell'audit IT è quella del risk assessment, ovvero l'analisi e valutazione dei rischi, effettuata attraverso una revisione dell'organizzazione IT della società al fine di rilevare le criticità che potrebbero compromettere la sicurezza della rete e dei dati. È utilizzata per decidere quali contromisure adottare al fine di rendere il rischio accettabile, in base all'importanza che una determinata risorsa informativa ha per l'azienda.

La gestione del rischio è un requisito essenziale dei moderni sistemi IT in cui la sicurezza è fondamentale; può essere definito come un processo nel quale si procede innanzitutto all'identificazione delle fonti di rischio, in seguito avviene una valutazione di queste ultime ed infine si sviluppano delle strategie per ridurle ad un livello accettabile. I tre obiettivi di sicurezza di qualsiasi organizzazione sono la riservatezza, l'integrità e la disponibilità dei dati. Durante un ciclo di audit è valutato se qualcuno di questi obiettivi viene violato e, in caso affermativo, fino a che punto (ISACA, 2016)[23].

La valutazione del rischio è una considerazione sistematica di:

- il danno aziendale che potrebbe derivare da un errore di sicurezza, tenendo conto le potenziali conseguenze di una perdita di riservatezza, integrità o disponibilità delle informazioni ed altre attività;
- una stima realistica della probabilità di avvenimento di un determinato fallimento al fine di prevedere minacce e vulnerabilità dei controlli attualmente implementati.

È necessario, in fase di pianificazione, analizzare il processo di gestione del rischio utilizzato dall'azienda al fine di comprendere quali minacce sono state identificate dal management, l'impatto che quest'ultime potrebbero avere sull'organizzazione e per dare una valutazione indipendente su come sono state affrontate e mitigate

[23] ISACA, *Information Systems Auditing: Tools and Techniques - Creating Audit Programs,* 2016

dall'amministrazione.

I passaggi che possono essere seguiti per la realizzazione di un piano di audit basato sul rischio (risk-based approach) sono:

- analizzare e classificare i sistemi informativi in uso nell'azienda;
- determinare quali di questi hanno impatto su funzioni o risorse critiche;
- valutare quali rischi incidono su questi sistemi e la gravità dell'impatto sul business;
- identificare quali controlli effettuare per affrontare i rischi IT rilevati e determinarne la frequenza.

I rischi che incidono su un sistema che dovrebbero essere presi in considerazione al momento della valutazione possono essere differenziati in: rischi intrinseci, rischi di controllo e rischi di rilevazione.

Il **rischio intrinseco** è la suscettibilità delle risorse di informazioni al furto di materiale, distruzione, divulgazione, modifica non autorizzata o altra perdita di valore. I controlli sono progettati per ridurre la possibilità che una minaccia sfrutti una vulnerabilità e provochi del danno.

Il r**ischio di controllo** consiste nel rischio che il controllo possa non essere efficace e, se non efficace, potrebbe derivarne una debolezza strutturale che si propaga su tutti i processi e informazioni che si basano sull'efficienza di quel controllo. I fattori che influenzano il rischio associato a un controllo sono:

- La natura e la rilevanza degli errori che il controllo intende prevenire o rilevare;
- Se ci sono stati cambiamenti, rispetto all'anno precedente, nel volume o nella natura delle transazioni che potrebbero influenzare negativamente il controllo e l'efficacia operativa;
- Se le informazioni gestite dal controllo hanno una storia di errori;
- La natura del controllo e la frequenza con cui opera;
- Il grado con cui il controllo si basa sull'efficacia di altri controlli (ad esempio, l'ambiente di controllo o altri controlli informatici generali);

- La competenza del personale che esegue il controllo o ne monitora le prestazioni, oppure se ci sono stati dei cambiamenti nel personale che opera sul controllo;
- Se il controllo si basa sulle prestazioni di un individuo o è automatizzato (ad esempio, i controlli automatici sono considerati generalmente meno rischiosi se i controlli generali informatici sono efficiaci) (PCAOB, 2007)[24].

Il **rischio di rilevazione** consiste nel rischio che le procedure che il revisore IT mette in atto non gli permettano di rilevare un errore.

Questi fattori incidono direttamente sull'entità del rischio di audit che può essere definito come rischio che la relazione informativa/ finanziaria possa contenere errori rilevanti che potrebbero non essere rilevati dell'audit.

Per essere supportati durante la fase di risk assessment vi sono dei framework che possono essere presi d'esempio per l'esecuzione della valutazione. Uno di questi è la matrice dei rischi e controlli, ovvero una lista che comprende i rischi più frequenti e i controlli che possono essere implementati al fine di mitigarli; tuttavia questi framework non devono essere utilizzati in maniera sistematica, ma devono essere impiegati come linee guida per la valutazione dei rischi, poiché nel singolo caso in esame potrebbe essere necessario includere nuovi rischi rispetto a quelli indicati dalla matrice, oppure dovrebbero essere modificati i controlli effettuati in base a come è gestito il processo all'interno dell'azienda in esame.

[24]Auditing Standard No. 5 - An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements: https://pcaobus.org/Standards/Archived/PreReorgStandards/Pages/Auditing_Standard_5.aspx

2.3 Understanding of controls

Successivamente alla fase di pianificazione, decisi quali saranno gli applicativi da analizzare e i controlli da testare, si procede con la fase di Understanding of Control, nella quale il team di audit IT ha l'obiettivo di capire come la società gestisce i processi e come sono implementati i controlli volti alla mitigazione dei rischi.

La valutazione dei controlli avviene solitamente in due modi:

- attraverso dei meeting tra il team di audit ed il personale della società revisionata durante i quali vengono analizzate e discusse le policy e procedure definite;
- oppure attraverso delle vere e proprie interviste con i vari application owner degli applicativi (ovvero dei dipendenti dell'azienda, solitamente del reparto IT, che si occupano in prima persona di gestire uno o più applicativi che sono sotto esame), che permetteranno di ottenere una migliore comprensione delle funzioni ed i controlli integrati all'interno del sistema.

Durante questi incontri l'obiettivo è quello di acquisire principalmente informazioni riguardo a:

- come si eseguono i controlli, ovvero la spiegazione passo per passo e le varie casistiche che si possono incontrare;
- quali dati sono utilizzati durante il controllo;
- come sono trattate le eccezioni;
- eventuali modifiche sostanziali che verranno eseguite sull'applicativo o sul controllo durante il periodo di audit (ad esempio se fosse previsto la sostituzione di un software in uso con un altro che opera in maniera diversa).

Le tipologie di controlli che sono verificate durante un audit IT sono 2: ITGC (IT General Controls) e i controlli applicativi, che comprendono gli ITAC (IT Application Controls) e gli ITDM (IT-dependet manual controls), inoltre vengono testate anche le IPE (Information Produced by Entity) che non sono dei controlli sugli applicativi, ma sono

delle informazioni prodotte dalla società (liste, report, tabelle, ecc) che verranno poi utilizzati sia dagli da personale interno all'azienda per concludere i controlli, sia dai revisori per effettuare i test, è quindi fondamentale che queste informazioni siano corrette e affidabili.

2.4 ITGC

I controlli generali sono alla base della struttura di controllo IT. Questi sono interessati all'ambiente generale in cui i sistemi IT sono sviluppati, gestiti e mantenuti. I controlli IT generali stabiliscono un quadro di verifica generale per le attività IT, sono le policies e le procedure utilizzate per supportare il corretto funzionamento delle applicazioni, dei controlli automatici in esse implementate, l'integrità dei numerosi report generati durante il funzionamento di quest'ultime e la sicurezza dei dati ospitati all'interno delle stesse.

Gli ITGC permettono di valutare il livello minimo di sicurezza che deve essere garantito nella progettazione e gestione di un sistema informatico (baseline di sicurezza), al fine di assicurare:

- riservatezza: le informazioni e i dati elaborati sono accuratamente protetti dalla divulgazione non intenzionale;
- accuratezza: tutte le transazioni e i dati sono elaborati in maniera accurata e le informazioni che ne risultano sono corrette;
- completezza: le informazioni che sono il risultato del processamento dei dati e delle transazioni sono complete e non vengono persi dati durante i vari processi.

Gli ITGC insistono sui Sistemi Informativi di una Società e si articolano su due livelli:

- Layer Applicativo: relativo alla gestione del Sistema Informativo da analizzare.
- Layer Infrastrutturale: considera i supporti di ogni Applicativo, cioè il Sistema Operativo (SO) e il Database (DB). Si riferisce, inoltre, al Dominio, struttura di rete comune a tutti gli applicativi.

Gli ITGC riguardano 3 aree:

- **Manage Change**: controlli sulle modifiche, manutenzioni e aggiornamenti apportati agli applicativi IT e ad altri componenti rilevanti dell'ambiente IT. Verificano che siano state seguite le policy aziendali

- **Manage Access**: controlli che verificano che gli accessi all'ambiente IT siano effettuati solamente dagli utenti autorizzati e che tali utenti possano eseguire solamente azioni che siano compatibili con le autorizzazioni assegnategli.
- **Manage IT Operations**: controlli effettuati sulle applicazioni di elaborazione e archiviazione dei dati che verificano che le informazioni trattate siano mantenute integre e che le elaborazione siano state eseguite correttamente.

Il processo di Manage Change considera le seguenti tipologie di cambiamenti:

- Manutenzione ordinaria dei sistemi;
- Modifiche ai programmi esistenti;
- Sviluppo di nuove funzionalità;
- Cambiamenti di emergenza;

Le varie modifiche effettuate possono avere delle priorità e dei livelli di rischio differenti, in base alle quali si seguono diverse procedure, ad esempio una modifica di un campo dell'interfaccia grafica di un applicativo ha un livello di rischio molto inferiore all'implementazione di una nuova funzionalità nel sistema, quindi l'azienda potrebbe avere delle procedure diverse per le due tipologie di modifica.

I principali rischi che si possono incontrare in un processo di Manage Change sono:

- I nuovi applicativi IT o le modifiche ai programmi esistenti non funzionano come descritto o richiesto perché non sono adeguatamente testati dalla persona appropriata;
- Le modifiche non sono state apportate da personale autorizzato;
- Non è rispettata la corretta segregation of duties (SoD) prevista durante il processo di modifica del sistema.

I processi di Manage Access mirano a controllare che nell'organizzazione in esame siano ben definiti i ruoli degli utenti e verificano le responsabilità associate alle varie utenze. È fondamentale che siano rispettate delle adeguate SoD in modo che i vari utenti abbiano dei privilegi d'accesso limitati a quelli necessari per permettergli di

svolgere le loro mansioni, altrimenti, potrebbero avere dei comportamenti fraudolenti nei confronti della società. I controlli si focalizzano su:

- Password policy: Individuazione delle parametrizzazioni di sicurezza adottate per confrontarle con le checklist di sicurezza definite dalla società che effettua l'audit per verificare l'adeguamento alle misure minime di sicurezza.
- Utenze aventi ampi privilegi: verifica che le utenze senza restrizioni siano un numero limitato e che siano attribuite soltanto a personale autorizzato in base alle mansioni aziendali svolte
- Creazione/ modifica utenze: verifica che il processo di creazione o modifica delle utenze segua il corretto iter di autorizzazioni;
- Terminazione delle utenze: verifica che il processo di creazione o modifica delle utenze segua il corretto iter di autorizzazioni e verifica sull'effettiva terminazione dell'utenza del personale che ha cessato di utilizzare un determinato applicativo;
- SoD: verifica della corretta segregazione delle funzioni. In particolare, verifica che, per le utenze create e modificate, i processi di richiesta, approvazione e creazione di un'utenza siano gestite da persone diverse, con le corrette autorizzazioni.

Infine, i processi di Manage IT Operations si concentrano a verificare che l'azienda in esame abbia un ambiente di elaborazione dei dati affidabile. Questo si ottiene sia verificando che le applicazioni adibite all'ottenimento dei backup delle informazioni funzionino in maniera corretta, sia assicurandosi che i sistemi di immagazzinamento di questi dati non siano soggetti ad attacchi informatici o deperimenti fisici. I controlli verificano che:

- I backup vengono eseguiti periodicamente tramite software appositi e monitorati dal personale IT per verificare il completamento e la risoluzione corretta di eventuali errori di backup;
- L'accesso al job scheduler sia limitato al personale autorizzato;
- I job automatici vengono eseguiti e monitorati correttamente al fine di gestire tempestivamente eventuali errori.

2.5 Test dei controlli ITGC

L'attività di verifica dei controlli ITGC avviene in due fasi, la prima è quella di WTT (Walk-Through Test) necessaria alla comprensione di come i controlli vengono implementati, mentre la seconda è quella di Test (Test of Effectiveness), nella quale viene verificata la vera e propria efficacia del controllo sul sistema informativo.

2.5.1 WTT

Questa fase serve all'auditor per analizzare il "design of control", cioè per valutare se il controllo è stato definito e disegnato in maniera efficace, nel caso in cui vengano intercettate delle mancanze o il disegno risultasse non adeguato per indirizzare tutti i rischi relativi, allora verrebbe rilevata una deficiency di disegno.

Durante questa operazione si utilizzano le informazioni ottenute mediante la fase di understanding. Attraverso queste risorse si comprende qual è la persona addetta allo svolgimento del controllo, in che modo è mitigato il rischio e la frequenza del controllo stesso all'interno dell'organizzazione, che può essere giornaliera, settimanale, mensile, ecc. Ottenute queste informazioni si procede passo per passo all'esecuzione del controllo, ad esempio il processo di creazione di un'utenza su un applicativo, così da verificare che il controllo sia strutturato in maniera efficace per mitigare i rischi per cui è predisposto.

Testata l'efficacia del disegno del controllo si procede con la fase di test nella quale viene valutata l'efficacia operativa dell'esecuzione del controllo da parte dell'azienda.

2.5.2 Test

In seguito alla fase di WTT si effettua quella di Test of Effectiveness (ToE), durante la quale si realizza la valutazione dell'operatività del controllo su un campione di item, dunque si verifica che quest'ultimo funzioni come dichiarato e riscontrato nella fase di disegno, ovvero si controlla che siano stati seguiti tutti i passi descritti nel disegno del controllo, per capire se il controllo risulta effective o ineffective.

Per testare l'efficacia di un determinato controllo si richiede all'azienda revisionata di fornire tutta la popolazione di item, relativa all'anno in cui viene effettuato l'audit. In base alla dimensione totale della popolazione si effettua un campionamento, ovvero si estraggono casualmente un numero di item e per questi ultimi si richiedono al cliente le evidenze dei controlli che sono stati effettuati. Attraverso questi documenti il revisore IT verifica che siano stati seguiti i vari passi descritti dal disegno del controllo. Il campionamento permette di fare delle valutazioni con un alto livello di confidenza, senza dover effettuare la revisione di tutti gli item della popolazione, che in alcuni casi potrebbe impiegare tempi molto prolungati, ad esempio un'azienda, in un anno, potrebbe avere più di 1000 modifiche su un applicativo. Tuttavia, dal campionamento sorge un rischio, ovvero che la conclusione dell'auditor sull'efficacia del controllo basata sul campione possa essere diversa di quella basata sull'intera popolazione. Le metodologie di audit tendono a diminuire questo rischio effettuando campionamenti con un elevato intervallo di confidenza.

Un controllo è considerato efficace se funziona come descritto nel disegno. Se durante la fase di test si notano delle eccezioni, ad esempio qualche passo descritto nel disegno del controllo non eseguito correttamente, l'auditor ha il compito di indagare con l'azienda sul motivo per cui non si è seguito perfettamente il disegno del controllo e deve valutare se l'eccezione rende il controllo ineffective o no. Testati tutti gli elementi del campione, se il revisore è riuscito a riprodurre il controllo effettuato dalla società eseguendo in maniera indipendente tutti i passi ed è riuscito ad ottenere lo stesso risultato, allora il controllo sarò effective.

Nel documento finale nel quale si riassume il controllo il revisore dovrà indicare:

- Il periodo di tempo coperto dal test;
- Descrizione del controllo;
- La numerosità della popolazione e del campione;
- La frequenza del controllo;
- Eventuali eccezioni incontrate durante il test ed eventuale dichiarazione che dimostra che le eccezioni trovate non invalidino il controllo;

- Conclusioni sulla qualità del controllo.

In seguito alla prima fase di test che copre un determinato periodo dell'anno vi è una seconda fase, quella di update test, che serve a verificare che nulla sia cambiato nelle procedure seguite dall'azienda nel periodo che intercorre dalla data di test alla fine dell'anno. Questa fase può essere svolta con differenti metodologie, dipende dal periodo di tempo che si vuole coprire. Più il periodo è lungo più è necessario svolgere dei test aggiuntivi, in alternativa sarà sufficiente ricevere conferma che i processi ed i controlli analizzati non abbiano subito modifiche successivamente alle valutazioni di test eseguite.

Nel caso in cui si riscontrasse un problema con un controllo significherebbe che uno o più rischi legati a un processo di un applicativo rimarrebbero scoperti e ne risulterebbe una deficiency. Le deficiencies negli ITGC possono ostacolare la capacità del management di ottenere informazioni finanziarie accurate. Se queste non venissero identificate ed affrontate in modo tempestivo, potrebbero compromettere il funzionamento dei controlli interni, con un impatto sulle decisioni interne (Deloitte, 2018) [25].

La deficiency può essere:

- nel design di un controllo ovvero quando manca un passaggio necessario a raggiungere l'obiettivo di controllo o un controllo esistente non è progettato correttamente in modo tale che, anche se il controllo funziona come previsto, l'obiettivo di controllo non verrebbe raggiunto. Questo tipo di deficiencies si individuano durante la fase di WTT;
- di tipo operativo, quando un controllo adeguatamente progettato non funziona come previsto, o quando la persona che esegue il controllo non possiede

[25] *General IT Controls*, Deloitte: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-general-it-controls-noexp.pdf

l'autorità o la competenza necessarie per eseguire il controllo in modo efficace. Queste sono invece rilevate durante la fase di test (PCAOB, 2007)[26].

In presenza di una deficiency il controllo non è considerato subito ineffective, ma è necessario effettuare ulteriori analisi per comprendere l'effetto di queste mancanze sui rischi relativi a un determinato controllo.

Innanzitutto, quando si incontra un'eccezione nei controlli è necessario:

- effettuare indagini specifiche e indagare sulla natura e sulla causa dell'eccezione;
- determinare se l'eccezione è sistematica o casuale:
- valutare l'effetto dell'eccezione sulle procedure di audit pianificate e su altre aree dell'audit.

Quindi è necessario stabilire se un'eccezione dell'attributo di un controllo ITGC è un'eccezione di controllo. Alcuni controlli generali IT hanno più attributi. Quando un attributo è insufficiente, si verifica se tale insufficienza causa l'insufficienza dell'intero controllo. Quando il problema relativo all'attributo impedisce al controllo di affrontare sostanzialmente il rischio, valutiamo il controllo come ineffective. Quando il problema relativo all'attributo di controllo non è così significativo da influire sull'utilità complessiva del controllo per affrontare il rischio, valutiamo il controllo come effective e documentiamo il motivo per cui l'attributo insufficiente non causa l'insufficienza dell'intero controllo. In seguito alla presenza di deficency è anche possibile effettuare il test di sostanza sul controllo, ovvero invece che testare solamente un campione della popolazione si effettua il test di tutta la popolazione così da verificare effettivamente se l'eccezione trovata è sistematica oppure un caso isolato.

[26] *Auditing Standard No. 5 - An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements:* *https://pcaobus.org/Standards/Archived/PreReorgStandards/Pages/Auditing_Standard_5_Appendix_A.aspx*

2.5.3 Valutazione dell'ITGC e dei processi sottostanti

Nella fase successiva si valutano i risultati dei test sugli ITGC e si determina se forniscono ragionevoli garanzie circa l'efficacia operativa degli ITGC pertinenti. Vengono eseguite le seguenti valutazioni relative ai controlli e ai rischi IT:

- ITGC operating evaluation: in base ai risultati dei test, viene effettuata una valutazione operativa per ciascun ITGC (vale a dire, ITGC è effective o ineffective). Nel caso un ITGC venga valutato come ineffective è possibile che i rischi correlati ad esso vengano mitigati anche da altri controlli, ovvero dai controlli compensativi;
- IT process evaluation: le valutazioni degli ITGC e / o qualsiasi test di sostanza eseguito vengono utilizzate per trarre una conclusione per verificare che ciascun processo IT rilevante affronti adeguatamente i rischi in tale processo. Queste valutazioni vengono utilizzate per determinare se i controlli ITAC e ITDM possono affidarsi alle informazioni generate dai processi correlati e per determinare l'entità del lavoro che verrà svolto sulle IPE. Le possibili valutazioni dei processi IT sono:
    - Effective: gli ITGC per il processo IT hanno funzionato efficacemente durante il periodo di audit
    - Reliable: è stato effetutato il test di sostanza per verificare ITGC ineffective
    - Ineffective: sono stati rilevati ITGC efficaci insufficienti e i test di sostanza, se effettuati, non possono fornire prove sufficienti per stabilire chi i rischi siano mitigati;

- Aggregate IT evaluation: le valutazioni IT aggregate riflettono l'effetto delle valutazioni dei controlli ITGC su ciascun ITAC e controllo ITDM supportato dall'applicazione IT nell'ambito. Le possibili valutazioni sono:

- Support: i processi IT sono stati valutati come effective o reliable, ovvero il funzionamento completo e accurato degli ITAC il funzionamento completo e accurato della parte automatizzata del controllo ITDM è supportato dal processo o dai processi IT correlati;
- Not Support: i processi IT sono stati valutati come ineffective, ovvero il funzionamento completo e accurato degli ITAC e degli ITDM non è supportato dal processo o dai processi IT correlati.

2.6 Controlli Applicativi

I controlli applicativi si applicano solo ai processi di business che essi supportano. Sono controlli designati all'interno delle applicazioni per prevenire o rilevare transazioni non autorizzate e supportare gli obiettivi di natura finanziaria quali la completezza, l'accuratezza, l'autorizzazione e la validità dei dati utilizzati per la predisposizione del bilancio (AIEA, 2006)[27]

I controlli applicativi si dividono in due categorie. Gli ITAC: sono controlli automatici eseguiti dai sistemi applicativi della società, che non richiedono un intervento manuale per la loro esecuzione. Solitamente utilizzati per il controllo di processi relativi all'avvio, registrazione, elaborazione e reportistica di transazioni o altri dati finanziari. Sono effettuati dal computer e funzionano sempre come sono stati definiti e non sono soggetti a errori intermittenti. Alcuni esempi sono:

- attività di controllo di quadratura: sono costituite da controlli che rilevano errori nell'inserimento dei dati attraverso la riconciliazione dell'ammontare acquisito manualmente o automaticamente con un totale di riferimento. Ad esempio, un'azienda riscontra automaticamente il numero totale delle transazioni elaborate e passate dal suo sistema di registrazione degli ordini online al numero di transazioni ricevute nel suo sistema di fatturazione;
- codici di controllo: un algoritmo per validare i dati. I codici degli articoli di un'azienda contengono un carattere di controllo per rilevare e correggere ordini non accurati inoltrati ai suoi fornitori. I codici di prodotto universali includono un codice di controllo per verificare il prodotto e il venditore;
- liste predefinite di dati: controlli che forniscono all'utente liste predefinite di dati accettabili.
- test di ragionevolezza dei dati: sono test che comparano i dati acquisiti con un campione di riferimento fisso o parametrizzato per la ragionevolezza dei dati in esame.;

[27] *Obiettivi di controllo IT per il Sarbanes – Oxley Act -2ª edizione*

- test logici: sono relativi all'uso di limiti di intervallo (range) o test sul tipo di dati (numerico/alfanumerico).
- calcoli: algoritmi numerici applicati da una routine automatica implementata all'interno delle applicazioni.

Gli ITDM (detti anche ibridi) sono essenzialmente dei controlli che hanno sia una componente manuale, sia una componente automatica. I report generati dal sistema sono normalmente basati su controlli ibridi, poiché forniscono i dati per la revisione del management. Per citare un esempio, la valutazione dei crediti verso i clienti può includere un controllo dove i manager revisionano, per valutarne la ragionevolezza, il report mensile delle scadenze. In questo esempio, un report viene prodotto dalla contabilità clienti (processo automatizzato) e rivisto per la relativa ragionevolezza (processo manuale).

I controlli applicativi sono testati per determinare se sono progettati, implementati e funzionanti in modo efficace.

2.7 Test dei Controlli Applicativi

Il test dei controlli applicativi deve essere eseguito per tutti i potenziali scenari che si possono configurare, eseguendo sia un test 'positivo' che un test 'negativo'.

Gli scenari sono tutte le possibili casistiche che devono essere verificate e che possono essere configurate all'interno del controllo. Ad esempio, se un controllo ha impatto su 5 tipologie di ordini di acquisto, l'application control andrà verificato per tutte le tipologie di ordine indicate al fine di verificarne l'omogeneità di comportamento.

Positive test: verifica del normale comportamento del sistema a seguito di un input atteso. Il fine della verifica è rilevare il corretto funzionamento del controllo a fronte in un input atteso dal sistema. Se viene rilevato un comportamento inatteso durante il test positivo, il test fallisce.

Negative test: verifica effettuata al fine di analizzare il comportamento dell'applicativo a fronte di input non attesi dal sistema. Il test negativo assicura che l'applicativo riesca a gestire dati non validi o comportamenti imprevisti da parte degli utenti.

L'attività di test dei controlli applicativi deve, inoltre, far emergere situazioni nelle quali è possibile effettuare un override del controllo stesso, ovvero la possibilità di riuscire ad alterare il funzionamento del controllo applicativo e quindi modificare l'efficacia del controllo.

Ad esempio, se in un controllo sono previste delle soglie di tolleranza, va indagato chi può modificare questi limiti senza che vi sia un controllo su tali modifiche. In caso di rilevamento di possibili azioni che permettano l'override, dovranno essere documentate le attività svolte dal management al fine di monitorare transazioni o funzionalità che permettono di rendere inefficace il controllo automatico.

Un esempio di test di controllo ITAC potrebbe essere su un applicativo di gestione delle fatture, che verifica che le fatture siano automaticamente generate dopo la vendita di prodotti finiti.

Il positive test consiste nei seguenti step:

- Creazione di un'uscita di merci per un prodotto finito;
- Verifica della creazione della fattura in seguito ad un'uscita merci;
- Verifica che i dati di fatturazione corrispondano a quelli dell'uscita merci del prodotto finito.

Il negative test si sviluppa come segue:

- Creazione di una fattura per un prodotto finito in assenza di un'uscita merci;
- Verifica che il sistema blocchi automaticamente la generazione di una fattura non legata ad alcuna uscita merci di prodotto finito.

Se entrambe le verifiche si concludono positivamente il controllo può essere considerato effective.

2.8 Information Produced by the Entity

Una IPE, Information Produced by the Entity, è una qualunque informazione prodotta dalla società per essere utilizzata durante i propri controlli, oppure per essere consegnata al revisore per permettergli di effettuare l'attività di test dei controlli. Sono generate usando gli applicativi IT, strumenti di end user computing (EUC, elaborazione da parte degli utenti tramite Excel o PowerPoint) o altri mezzi (inclusa la preparazione manuale della documentazione). Le IPE possono essere sia informazioni di tipo finanziario sia di tipo non finanziario, ciò che identifica l'IPE non è il tipo di informazione, ma chi l'ha prodotta, ovvero qualcuno all'interno dell'azienda, che sia una persona fisica oppure un sistema informativo; le IPE sono anche create dalle società di servizi, ovvero quelle società che offrono all'azienda auditata dei servizi che sono rilevanti per i sistemi informativi e che producono delle informazioni. Ad esempio, l'organizzazione assunta per gestire ed elaborare le buste paga per conto dell'azienda è un'organizzazione di servizi. Per questi motivi non è sempre facile individuare tutte le IPE e ciò potrebbe creare problemi perché durante l'audit potrebbero non essere identificati tutti i rischi derivanti dall'utilizzo e dalla generazione di questo tipo d' informazioni.

I rischi relativi alle IPE sono prevalentemente 6:

1. I dati elaborati dall'applicazione IT da cui viene prodotto l'IPE non sono completi o accurati;
2. I dati estratti dall'applicazione IT nell'IPE non sono i dati richiesti o non sono completi;
3. I parametri inseriti dall'utente sono inappropriati;
4. I calcoli o le categorizzazioni eseguiti nella creazione dell'IPE non sono accurati;
5. L'output dei dati dall'applicazione allo strumento EUC viene modificato o perso nel trasferimento;
6. Le informazioni aggiunte o modificate (inclusi nuovi calcoli e categorizzazioni) utilizzando lo strumento EUC sono incomplete, inesatte o inadeguate.

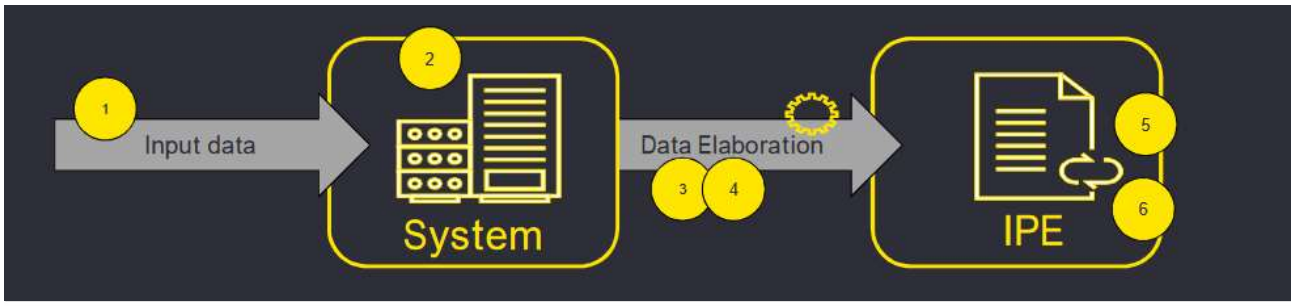


Figura 1: processo di creazione di un'IPE e rischi associati

Per le IPE create da un'applicazione IT che viene trasmessa a uno strumento EUC, i rischi di completezza ed accuratezza possono essere raggruppati in tre macrocategorie:

- Underlying data: in che modo i dati utilizzati per creare l'IPE sono stati inseriti ed elaborati nell'applicazione IT (rischio 1). Si considera che i dati utilizzati dall'applicativo per generare la IPE possano essere errati e dunque quest'errore si potrebbe propagare lungo il processo di utilizzo dell'IPE e dunque sui test dei controlli;
- IPE definition program: il programma di definizione IPE è il programma per computer che viene eseguito quando un utente richiede informazioni dal database di un'applicazione IT. Il programma definisce le informazioni da estrarre dai dati che sono stati raccolti e definisce il modo in cui tali informazioni debbano essere presentate all'utente. Bisogna tenere in considerazione che il programma estragga correttamente le informazioni richieste dal database e verificare il modo in cui le organizza e le presenta all'utente (rischi 2 e 4);
- User actions: le azioni dell'utente possono influenzare l'IPE in tre modi. Innanzitutto, l'utente può inserire i parametri in un programma di definizione IPE, quindi bisogna verificare che nell'inserimento di quest'ultimi non sono stati commessi errori. In secondo luogo, quando l'output del programma di definizione IPE viene esportato in uno strumento EUC, sono necessarie delle azioni di verifica da parte dell'utente per constatare che non vi siano state omissioni durante il processo di esportazione dei dati. In terzo luogo, una volta

che l'IPE si trova in uno strumento EUC, l'utente è libero di manipolare, aggiungere o eliminare i dati come desidera. Se l'IPE viene creato interamente in uno strumento EUC (ovvero, le informazioni non sono un'esportazione da un'applicazione IT), l'utente ha pieno controllo sulle informazioni contenute nella IPE (rischi 3, 5, 6).

Quindi, dal momento che le IPE saranno utilizzate per effettuare delle valutazioni in merito all'adeguatezza dei controlli interni dell'azienda, è essenziale che anche queste ultime abbiano dei controlli atti a verificarne la consistenza e che questi vengano testati al fine di verificare che funzionino correttamente

I test delle IPE sono svolti in base al fatto che esse siano generate da applicativi IT già testati e valutati come effective, oppure no.
Se un'IPE è prodotta da un sistema IT già testato e sicuro allora i controlli a copertura dei rischi prettamente IT (rischi 1, 2 e 4), verranno valutati una sola volta all'interno di un ciclo di audit e verrà controllata la consistenza d accuratezza dei dati estratti (i restanti rischi essendo di carattere manuale dovranno invece essere indirizzati da controlli svolti ogni qualvolta l'IPE viene utilizzata).
Quando invece le IPE sono generate da sistemi IT non verificati o verificati ma con risultati ineffective, oppure sono redatte manualmente dal personale dell'azienda, allora saranno testate ogni volta che verranno utilizzate per verificare sia che la fonte delle informazioni sia corretta, sia che siano state utilizzate le query e gli algoritmi corretti per estrarre i dati richiesti.
Anche le IPE, come i controlli, ricevono una valutazione da parte dell'auditor.

2.9 Opinion sul bilancio

Concluso il periodo di test sui controlli si passa all'ultima fase del ciclo di audit IT. Il team di revisione dei sistemi informativi è tenuto a redigere tutta la documentazione al fine di supportare il lavoro svolto e deve comunicare ai colleghi della revisione contabile i risultati ottenuti al fine di certificare l'affidabilità dei sistemi informatici con cui l'azienda manipola e gestisce le informazioni contabili.
Una volta ottenuta l'informativa a riguardo dell'efficienza del sistema di controlli IT interno ed in seguito alle procedure volte a verificare la veridicità dei dati contenuti nel bilancio, il team di revisori deve fornire un'opinione sull'efficacia del controllo interno sulla rendicontazione finanziaria valutando le prove ottenute da tutte le fonti, gli errori rilevati durante la revisione contabile e qualsiasi carenza di controllo identificata.
Il giudizio della società di revisione in merito al bilancio della società in esame avviene attraverso una relazione redatta in forma di lettera, i cui destinatari sono i soci. Questa lettera si articola in tre paragrafi: il primo identifica il bilancio assoggettato alla società di revisione contabile ed assegna le rispettive responsabilità degli amministratori della società e del revisore; nel secondo sono identificati i principi di revisione di riferimento e vengono illustrate sommariamente le procedure adottate; il terzo paragrafo esprime il giudizio del revisore sulla conformità del bilancio rispetto ai principi contabili di riferimento e si esprime sulla chiarezza della redazione nonché sulla veridicità e correttezza della rappresentazione della situazione patrimoniale e finanziaria e del risultato economico della società. La lettera infine viene firmata dal partner della società di revisione e così si conclude il ciclo di audit. (L'Appendice 1 mostra un esempio di lettera di opinion della società Ernst&Young riguardante la revisione del bilancio del gruppo ACEA per il Fiscal Year 2013).

Capitolo 3

Nel periodo compreso tra il 03 Febbraio 2020 e il 30 Aprile 2020 ho svolto uno stage curriculare presso l'ufficio di Torino dell'azienda EY Advisory S.p.a. facente parte del network Ernst&Young, , che, insieme a Deloitte & Touche, Pricewaterhouse Coopers e KPMG, fanno parte delle così dette Big Four, ovvero le più grandi aziende di revisione contabile sul mercato.

EY è una società con oltre 280.000 dipendenti, che possiede circa 700 uffici in tutto il mondo, suddivisi in tre regioni geografiche: Americhe, EMEIA (Europe, Middle East, and Africa) e Asia-Pacifico, che nel 2019 ha fatturato ricavi per 36,4 miliardi di dollari, ottenendo una crescita di circa 8% rispetto all'anno precedente, dimostrandosi così una società in forte crescita (EY, 2020).

L'azienda offre quattro service line differenti:

- Assurance: servizi che si occupano di aiutare le aziende di rispondere ai fabbisogni informativi che derivano dai mercati, il dominio principale è quello della revisione legale dei conti;
- Advisory: servizi offerti alle aziende per migliorare le proprie performance utilizzando le nuove tecnologie e per gestire correttamente i rischi;
- Tax: servizi riguardanti le aree della fiscalità e del diritto societario che aiutano le aziende a stare dietro ai continui cambiamenti nella legislazione;
- Transaction Advisory: servizi di consulenza che guidano i clienti durante le operazioni di M&A (EY, 2019).

Come si può osservare nelle Appendici 2 e 3 le Service Line di Assurance e Advisory sono quelle che hanno generato più ricavi per l'azienda e che hanno occupato più dipendenti nel 2019, infatti hanno contribuito rispettivamente al 34,7% e 28,1% dei ricavi totali e hanno occupato il 33,2% e il 23,8% dei dipendenti totali.

EY S.p.a. è una società che sta crescendo molto, come tutte le aziende che si occupano di revisione di bilancio, vista la crescente attenzione che ha ricevuto questa disciplina

negli ultimi decenni. Tra i clienti che si sono affidati a EY nel 2019 spiccano i 141 Enti di Interesse Pubblico i cui bilanci e sistemi informativi sono stati oggetto di revisione legale[28] (EY, 2019), alcuni di questi, come FCA Bank S.p.A., Juventus Football Club S.p.A. e CALEFFI S.p.A. (EY, 2019) sono stati revisionati proprio dall'ufficio di Torino.(In Appendice 1 sono elencate tutti gli EIP che sono stati seguiti da EY nel 2019).

I clienti all'interno della società sono suddivisi in: piccoli, medi e grandi, in base a quante risorse saranno necessarie, quanto tempo dovrà essere impiegato per completare il processo di revisione e al budget che è stato stanziato per un determinato progetto.

[28] EY, *Relazione di Trasparenza 2019*

3.1 Obiettivi del tirocinio

L'obiettivo del tirocinio era quello di inserirmi all'interno del contesto delle società di consulenza, più precisamente la revisione dei sistemi informativi a supporto della revisione contabile e di presentarmi quali fossero i ruoli e le responsabilità dell'IT auditor all'interno della società stessa e nei confronti dei clienti. Innanzitutto, mi è stato spiegato quali fossero i compiti e gli obiettivi perseguiti dall'IT audit, essendo a me un mondo estraneo. Mi è stato illustrato il funzionamento di un piano di audit: dall'acquisizione del cliente, che è responsabilità dei partner e avviene tramite gare di appalto, fino alla conclusione del progetto che avviene tramite la lettera di relazione di revisione del bilancio e dei sistemi informativi. In seguito, sono stato affiancato ad un Senior Consultant, una figura con qualche anno di esperienza all'interno del settore, e da un manager, che hanno avuto il compito di formarmi al fine di poter affrontare un progetto di audit. Mi è stato introdotto EY Canvas, le piattaforma online, che opera sul cloud privato dell'azienda, con la quale all'interno di EY sono gestiti i vari progetti di audit, il quel mette in collegamento i dipendenti con i clienti e sulla quale sono caricati i report definitivi dei lavori effettuati per ogni singolo progetto[29] (EY, s.d.). Inoltre, questo tool permette ad ogni dipendente di sapere quali sono le proprie attività e la percentuale di completamento dei lavori che sta seguendo.

In seguito, ho ricevuto una panoramica sugli strumenti che avrei adoperato durante le mie attività, alcuni dei quali conoscevo già ampiamente, come il pacchetto office, altri che sono specifici per le attività di audit, come ACL (Audit Command Language), un tool di analytic che è in grado di manipolare una quantità di dati molto più elevata rispetto ai normali fogli di calcolo e permette di svolgere delle analisi più approfondite. Inoltre, ho dovuto apprendere la metodologia di revisione e risk management sviluppata da EY, basata sugli standard forniti dalla SEC, dal PCAOB e dall'IIA, alla quale avrei dovuto fare riferimento durante il processo di revisione dei sistemi informativi; infine mi è

[29] *EY Canvas,* EY: https://www.ey.com/en_gl/audit/technology/canvas

stato insegnato qual è il valore che EY vuole assegnare al cliente e di conseguenza come ci si deve comportare con essi durante lo svolgimento dell'attività lavorativa.

Il ruolo che sono andato a ricoprire è stato quello di consulente informatico all'interno del dominio "Technology Risk" della service line Advisory, il cui obiettivo è quello di occuparsi di attività e progetti di gestione del rischio in ambito tecnologico e assicurare alle aziende il corretto supporto per il rispetto della governance IT e compliance IT. Nello specifico sono stato inserito all'interno dei progetti di IT audit.

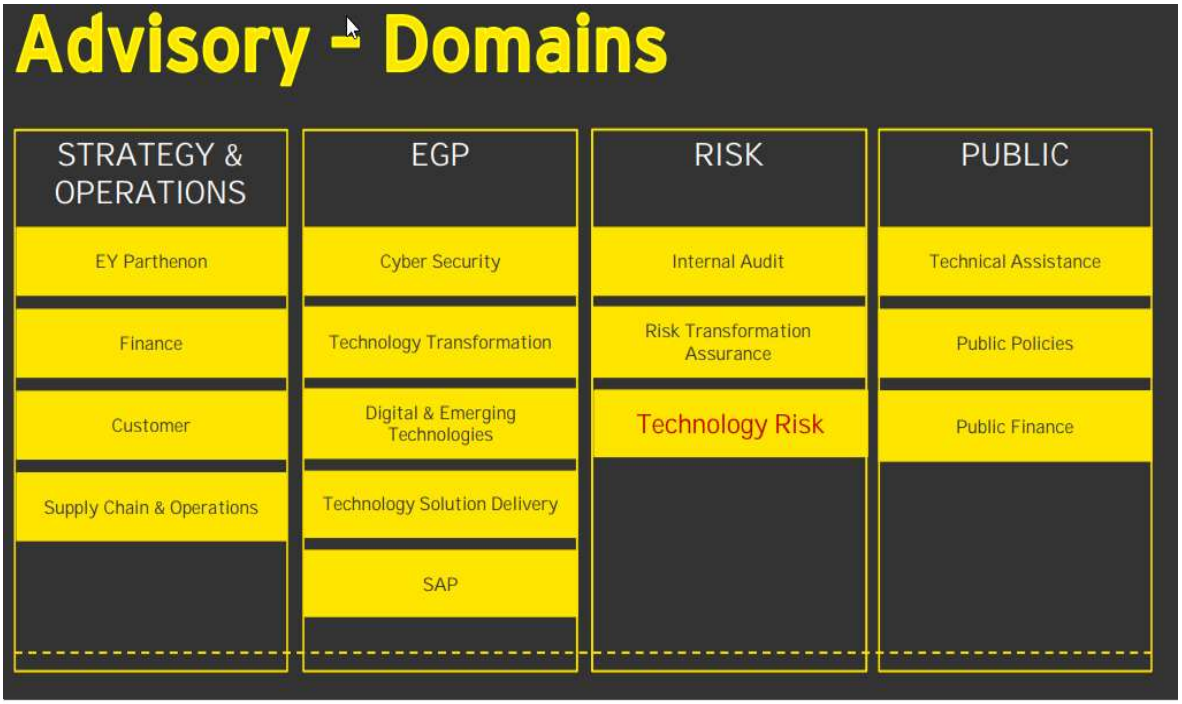


Figura 1: domini della service line Advisory

3.2 Introduzione nell'azienda

Il Team di IT audit dell'ufficio nel quale ho svolto lo stage curriculare era composto da 13 membri: un Senior Manager, due Manager, tre Senior consultant e 7 membri staff (tra cui il sottoscritto, unico tirocinante). Internamente vi era un'ulteriore suddivisione in due sottogruppi i cui membri erano assegnati agli stessi progetti, con le dovute limitazioni dettate dalle dimensioni dell'azienda cliente, entrambi diretti dell'unico Senior Manager. Io sono stato inserito nel team al quale apparteneva il mio tutor aziendale (Manager) e il Senior consultant ai quali ero stato affiancato per la mia formazione; queste due persone sono state il mio punto di riferimento all'interno dell'azienda.

Durante la prima settimana di lavoro mi è stata introdotta l'azienda (le metodologie e gli strumenti da utilizzare e i valori etici che guidano la società) ed è iniziata la mia formazione come IT auditor, sia attraverso dei corsi telematici offerti dall'azienda e realizzati appositamente per i nuovi assunti, sia attraverso l'osservazione delle attività che avrei dovuto svolgere e l'analisi dei progetti degli anni passati. In seguito a questo periodo di formazione, che è durato circa una decina di giorni, sono stato messo a disposizione del mio team come risorsa supplementare, senza essere assegnato a un progetto in particolare, poiché il periodo nel quale sono entrato in azienda è cruciale per le società di consulenza perché è la fase dell'anno in cui sono chiusi i progetti dei clienti più grandi, quindi i carichi di lavoro, fino alla fine di febbraio sono molto pesanti. Dunque, avevo il compito di assistere i miei colleghi più sommersi dal lavoro poiché entro il 21/02 si sarebbe dovuto concludere un progetto di IT audit presso una grande società torinese. In questo periodo ho svolto attività prettamente operative e ripetitive, che non richiedono particolari capacità relative alla professione di revisore ma consumano molto tempo, sono tuttavia fondamentali per la conclusione del ciclo di audit; sostanzialmente ho dovuto scaricare dalla piattaforma EY Canvas tutti i report prodotti relativi ai test sui controlli effettuati dai miei colleghi e ho redatto un documento riassuntivo nel quale ho elencato per ogni applicativo in scopo le date in cui è stato effettuato l'inquiry con i responsabili IT dell'azienda cliente, quali test sui

controlli sono stati effettuati e le varie date di copertura di test e di upgrade test. Una volta concluso questo documento ho proceduto alla formalizzazione dei test dei controlli ITGC più semplici facendomi guidare da documenti dell'anno precedente e dalle mie competenze acquisite durante la formazione.

Durante questo periodo iniziale mi sono ritrovato un po' spiazzato, poiché nel giro di pochi giorni ho dovuto apprendere moltissime informazioni e procedure e mi è stato subito chiesto di mettertele in pratica, di conseguenza mi sono ritrovato a svolgere dei compiti per i quali non mi sentivo completamente preparato e di cui non comprendevo appieno le logiche di funzionamento. In seguito, avendo fatto notare questa mia situazione al Senior consultant a me assegnato ho scoperto essere una situazione completamente normale all'inizio dello stage e mi è stato detto che le cose sarebbero diventate sempre più chiare una volta metabolizzati i meccanismi su cui si basa il processo di IT audit.

3.3 Progetto di Audit IT di una società medio/piccola inserita nel mercato del "food and beverage"

Il giorno 25 febbraio sono stato assegnato, assieme ad alcuni membri del mio team ad un progetto che consisteva nella revisione dei sistemi informativi di una società torinese medio/piccola[30], che per motivi di segretezza aziendale resterà anonima ed in seguito mi riferirò ad essa come azienda X, che si inserisce all'interno del mercato del "food and beverage"; il progetto sarebbe dovuto terminare il 23 aprile, con la consegna della lettera di opinion da parte del partner di EY, tuttavia questa scadenza è stata posticipata in seguito a ritardi avvenuti a causa dell'emergenza sanitaria globale che è avvenuta in quei mesi; nonostante i ritardi causati dalle chiusure degli uffici del cliente il nostro team è stato in grado di terminare tutti i compiti assegnatigli nei tempi previsti all'inizio del progetto. Dalla fine di febbraio in poi i miei sforzi si sono concentrati prevalentemente su questo cliente, con dei focus su altri engagement solamente quando dei colleghi avevano bisogno di terminare dei lavori per via delle tempistiche ristrette.

Come descritto nel secondo capitolo la prima fase è stata effettuata dai colleghi della revisione contabile, che hanno individuato le SCOTs relative al bilancio del cliente, e hanno determinato quali fossero gli applicativi sui quali avremmo dovuto concentrare la nostra analisi, ovvero, in questo caso, solamente un SAP.

3.3.1 ITGC e comprensione dei processi di gestione IT

Identificato l'applicativo da analizzare abbiamo potuto procedere con i l'incontro con i referenti per il sistema in scopo; incontro che, in situazioni normali, viene svolto in prima persona, tuttavia, a causa dell'emergenza sanitaria, l'azienda X permetteva l'accesso ai suoi uffici solamente ad alcuni dipendenti interni, di conseguenza questio incontro è stato svolto attraverso i sistemi di teleconferenza.

[30] [30] Con il termine medio/piccola si intende dal punto di vista di un'audit, ovvero il numero di applicativi in scopo e la quantità di controlli da testa, non dal punto di vista legislativo che classifica la grandezza delle azienda dal punto di vista del numero di dipendenti e del fatturato.

Durante questa fase del processo di revisione dei sistemi informativi il nostro obiettivo era quello di capire come fosse strutturato l'ambiente IT nel quale è inserito l'applicativo, quali fossero i processi relativi ad esso, quali controlli fossero messi in atto al fine di minimizzare i rischi associati, la loro descrizione passo per passo, le persone che partecipano ai controlli e la frequenza con la quale sono effettuati, ad esempio il controllo su una nuova utenza non ha una frequenza fissa ma viene effettuato solamente quando vi è la creazione di un'utenza sull'applicativo, invece quello sulle policy delle password viene effettuato annualmente. Di conseguenza ci siamo fatti spiegare nel dettaglio i processi di:

- Manage Change (MC): ovvero le procedure e i controlli effettuati per portare una modifica sull'applicativo. Il processo che ci è stato spiegato è il seguente: deve essere creata una change request attraverso lo strumento di ticketing specifico per l'applicativo, nella quale viene spiegata l'esigenza; in seguito la richiesta della modifica deve essere approvata da personale autorizzato che provvede anche ad assegnare al team della Società esterna che ha in carico lo sviluppo delle modifiche per la società X. La Società esterna provvede a sviluppare la modifica e, una volta terminata, attende i risultati degli UAT (User Acceptance Test) da parte di utenti di business interessati dalla change, che dovranno valutare che la modifica eseguita sia in linea con la richiesta e funzioni in maniera appropriata. Se i test danno esito positivo viene autorizzato il passaggio della modifica in ambiente di produzione, altrimenti vengono richiesti ulteriori cambiamenti fino ad ottenere il risultato desiderato; il processo termina con l'effettivo passaggio in ambiente di produzione. In ambito di MC si controlla che sia rispettata la corretta SoD, ovvero che le persone che sviluppano una modifica siano diverse da quelle che la trasportano in produzione, questo viene fatto verificando semplicemente che coloro che hanno le autorizzazioni a lavorare in ambiente di sviluppo non abbiano i permessi per trasportare in produzione una modifica, oppure, nel caso in cui ci sia un utente che, per necessità interne, abbia entrambe le autorizzazioni, deve essere presente un attività di monitoraggio dei trasporti al fine di controllare che

nessuno abbia mai trasportato in produzione change non autorizzate. Infine, l'ultimo processo di MC riguarda la segregazione degli ambienti, ovvero che esistano almeno tre ambienti, uno di produzione, uno di test e uno di sviluppo, in modo tale che le modifiche non siano sviluppate direttamente nell'ambiente di produzione.

Per quanto riguarda i processi di Manage Change i rischi individuati e i controlli messi in atto, comprensivi di attributi da soddisfare per essere considerati effective sono elencati nella tabella seguente.

Rischio	Controllo	Attributi del controllo
Le nuove funzionalità dell'applicativo IT o le modifiche a quelle esistenti non funzionano come descritto o richiesto perché non sono adeguatamente testate da persone appropriate diverse dagli sviluppatori	MC1.1:Le modifiche ai programmi applicativi sono adeguatamente richieste, testate (UAT) e approvate prima di essere migrate in produzione.	A: EY ha verificato che la modifica è stata autorizzata prima di iniziare con lo sviluppo.
		B: EY ha verificato che la modifica è stata testata.
		C: EY ha verificato che la modifica è stata approvata dal responsabile dell'azienda appropriato.
		D: EY ha verificato che la modifica è stata spostata in produzione in seguito all'approvazione.
		E: EY ha verificato che il personale che ha sviluppato il cambiamento è diverso dal personale coinvolto nel passaggio al cambiamento in produzione.
I programmi in produzione non sono protetti, consentendo agli sviluppatori di spostare le modifiche non autorizzate o non testate nell'ambiente di produzione.	MC2.4: l'azienda identifica quali utenti possono accedere all'ambiente di sviluppo e quali possono accedere all'ambiente di produzione	A: EY ha ispezionato chi può accedere all'ambiente di sviluppo.
		B: EY ha ispezionato chi può accedere all'ambiente di produzione.
		C: EY ha verificato l'adeguatezza degli elenchi di utenti identificati negli attributi A e B.
		D: EY ha ispezionato il rispetto della separazione dei compiti tra l'attributo A e l'attributo B.
	MC2.8: Gli ambienti di sviluppo, test e produzione sono separati per le modifiche al livello dell'infrastruttura.	A: EY ha ispezionato l'esistenza di un ambiente diverso da quello di produzione.
Il personale IT verifca che non vi siano modifiche non autorizzate a sistemi o programmi (comprese interfacce, configurazioni e logica dei report	MC2.4: l'azienda identifica quali utenti possono accedere all'ambiente di sviluppo e quali possono accedere all'ambiente di produzione	A: EY ha ispezionato chi può accedere all'ambiente di sviluppo.
		B: EY ha ispezionato chi può accedere all'ambiente di produzione.
		C: EY ha verificato l'adeguatezza degli elenchi di utenti identificati negli attributi A e B.
		D: EY ha ispezionato il rispetto della separazione dei compiti tra l'attributo A e l'attributo B.
	MA3.7: Le super utenze IT sono limitate e in linea con le responsabilità lavorative.	A: EY ha verificato che le liste di partenza sono state completate
		B: EY ha verificato che gli utenti Super sono limitati
		C: EY Ispezionato che l'assegnazione degli utenti privilegiati è in linea con le responsabilità

Tabella 1: rischi e controlli associati ai processi di Manage Change

- Manage Access (MA): vale a dire il processo per la creazione, o modifica delle autorizzazioni di un'utenza su quell'applicativo, quali persone possono farne richiesta, come sono trattate le utenze dismesse, la presenza di super utenze con privilegi particolari (SUID), quali sono i parametri di accesso ed autenticazione all'applicativo. Il processo di creazione utenza che ci è stato descritto è a grandi linee il seguente: la richiesta deve essere effettuata tramite apposito strumento di ticketing nella quale si specifica che deve essere creata una nuova utenza per una determinata persona e quali permessi devono essergli assegnati, è anche possibile indicare un'utenza dalla quale copiare le autorizzazioni. La richiesta deve essere innanzitutto approvata, ed in seguito il personale apposito provvederà a crearla assegnandoli i ruoli richiesti ed approvati. Una volta creata l'utenza il richiedente verrà informato dell'avvenuta creazione.

  Il processo di terminazione utenze prevede che le utenze vengano disabilitate una volta che non sono più necessarie, ovvero quando un dipendente esce dalla società, oppure non ha più bisogno di un'utenza sull'applicativo poiché non avrà più necessità di lavorare su di esso.

  Per quanto riguarda i controlli sulle password policy e gli accessi all'applicativo ci sono state semplicemente indicati quali sono i requisiti delle password di autenticazione per accedere all'applicativo (lunghezza minima, massimo, presenza o meno di caratteri speciali, ogni quanto bisogna cambiare la password, ecc.).

  In merito alle SUID, le utenze super – user ad ampi privilegi che sono in grado di svolgere determinate attività critiche all'interno della società (creazione o modifica di un'utenza senza che vi sia la previa autorizzazione, applicare modifiche direttamente in produzione, modifica dei parametri di sicurezza), siamo andati a comprendere insieme ai referenti quali fossero i profili e i ruoli che permettessero di compiere queste attività, in modo da poter identificare chi tra il personale dell'azienda avesse questi privilegi e verificare che siano stati attribuiti a persone che, per motivazioni organizzative, avessero il ruolo

effettivo per poter svolgere questo tipo di attività. In linea generale tali abilitazioni consentendo di svolgere attività critiche all'interno del sistema dovrebbero essere assegnare ad un numero limitato di persone. I rischi individuati e i controlli messi in atto, comprensivi di attributi da soddisfare per essere considerati effective sono elencati nella tabella seguente.;

Rischio	Controllo	Attributi del controllo
Impostazioni di sicurezza e autenticazione inadeguate	MA1.1: Le password per le applicazioni e le configurazioni di sicurezza sono impostate in modo efficace.	A: EY ha verificato che le impostazioni della password e le impostazioni di sicurezza sono configurate in modo appropriato in base alle procedure / pratiche dell'azienda e in linea con le pratiche principali di EY
Gli utenti dell'ambiente IT non sono autorizzati perché: - Le richieste di rimozione degli accessi non necessari del personale IT non vengono presentate tempestivamente - Le richieste di azioni di accesso sono soddisfatte in modo impreciso o inopportuno	MA2.1: Nuove richieste di accesso, modifiche o cancellazioni all'applicazione sono adeguatamente approvate.	A: EY ha verificato che la richiesta di creazione/ modifica /eliminazione del nuovo utente è stata adeguatamente documentata.
		B: EY ha verificato che la creazione / modifica del nuovo utente viene eseguita dopo la richiesta e l'approvazione.
		C: EY ha verificato che soggetti diversi richiedono, autorizzano e creano il nuovo utente (esiste una separazione dei compiti incompatibili nell'ambiente di accesso logico)
		D: EY ha verificato che nessuno poteva approvare le richieste da solo
	MA2.2: viene verificato che il profilo richiesto è il profilo assegnato all'utente.	A: EY ha verificato che il profilo implementato è lo stesso profilo richiesto.
L'accesso degli utenti IT all'ambiente IT crea conflitti di separazione dei compiti	MA3.5: La società identifica utenti diversi e appropriati tra chi può richiedere / approvare la creazione / modifica / cancellazione degli utenti e chi ha i privilegi per svolgere questa attività.	A: EY ispezionato ogni responsabile dell'approvazione non è tra gli utenti che hanno i diritti di creare / modificare / cancellare altri account.
	MA3.7: Le super utenze IT sono limitate e in linea con le responsabilità lavorative.	A: EY ha verificato che le liste di partenza sono state completate
		B: EY ha verificato che gli utenti Super sono limitati
		C: EY Ispezionato che l'assegnazione degli utenti privilegiati è in linea con le responsabilità

Tabella 2: rischi e controlli associati ai processi di Manage Access

- Manage Operations (MO): ovvero con quali job automatici e sistemi di backup, sempre se presenti, si garantisce l'integrità e l'archiviazione delle informazioni prodotte, la loro schedulazione e come sono gestiti i "Disaster Recovery Plan".

Riguardo a questi processi i referenti della società X ci hanno semplicemente spiegato quali backup effettuassero e quali job automatici si riferissero agli applicativi in scopo, specificandone la schedulazione (giornaliera, settimanale, mensile) e la tipologia (online o offline). Per quanto riguarda i backup ci è stato riferito che l'azienda effettua due tipi di backup: uno online schedulato dal martedì al sabato e uno offline schedulato solamente il lunedì.
I job schedulati invece sono 10 ed hanno una frequenza giornaliera.

Rischio	Controllo	Attributi del controllo
Problemi con programmi che non possono arrivare a completamento non sono considerate o sono considerate in una maniera non appropriata	MO1.1: Garantire che i job critici delle applicazioni IT nell'ambiente di produzione siano monitorati e che i risultati imprevisti vengano opportunamente indirizzati.	A: EY ha verificato che la Società controlla l'esecuzione dei job con la frequenza appropriata.
		B: EY ha verificato che il personale coinvolto nel processo di monitoraggio dei job è appropriato.
		C: EY ha ispezionato che qualsiasi errore deio è preso in carico dal personale appropriato e risolto
Problemi hardware o software comportano la perdita di dati o l'impossibilità di accedere ai dati come richiesto	MO2.1: I backup vengono eseguiti periodicamente tramite software di backup e monitorati dal personale IT per verificare il completamento e la risoluzione corretta di eventuali errori di backup.	A: EY ha verificato che la Società monitora l'esecuzione del backup con la frequenza appropriata.
		B: EY ha verificato che il personale coinvolto nel processo di monitoraggio del backup è appropriato.
		C: EY ha verificato che qualsiasi errore del processo di backup sia preso in carico dal personale appropriato e quindi recuperato.

Tabella 3: rischi e controlli associati ai processi di Manage Operations

La comprensione del funzionamento dei processi sopra elencati è essenziale innanzitutto per verificare che l'azienda abbia implementato tutti i controlli necessari al fine di mitigare i rischi che potrebbero incorrere durante la quotidiana operatività e l'utilizzo dei sisitemi; in secondo luogo per poter effettuare le opportune verifiche al momento dei test sui controlli ITGC. Questi ultimi sono fondamentali, poiché una volta testati è possibile affermare, se gli esiti sono positivi, che per l'anno fiscale considerato, l'applicativo è sicuro e le procedure di controllo sono rispettate correttamente.
Alla fine di entrambi gli incontri abbiamo richiesto, per ogni controllo, un esempio che confermasse che effettivamente i processi funzionassero come ci avevano raccontato,

quindi per ogni attività descritta durante l'incontro ci sono state fornite delle evidenze, che avremmo utilizzato in seguito per verificare il "design of control". Le evidenze sono il mezzo con il quale EY può provare che i vari processi di gestione della funzione IT all'interno della Società revisionata siano poi effettivamente messi in atto. Le evidenze possono essere di diversa natura: scambi di mail, apertura e chiusura di ticket al sistema di supporto, print screen catturati direttamente sul sistema, ecc.; variano in base alla tipologia di processo e come questi vengono gestiti.
A valle degli incontri, come da procedura standard dell'azienda, abbiamo compilato dei documenti di word (uno per controllo) nei quali abbiamo riportato le procedure dei controlli che ci sono state spiegate dai referenti, con i relativi rischi mitigati. Questi documenti sono di fondamentale importanza, poiché descrivono il processo schematizzato passo per passo, con tutte le casistiche che possono essere incontrate e indicano quali persone, all'interno dell'azienda X, hanno la responsabilità di determinate fasi del controllo. Nel caso in cui tali evidenze confermassero quanto descritto durante gli incontri di walkthrough queste saranno poi utilizzate come base di partenza per le attività di test. Inoltre, permettono anche a persone che non hanno partecipato ai meeting con i referenti di poter effettuare i test sui controlli ITGC nel caso vi fosse bisogno di più personale sul progetto di audit.

3.3.2 Test of Design

All'interno della fase di Walkthrough troviamo la parte di comprensione dei processi descritta nel paragrafo precedente, nella quale abbiamo compreso quali fossero i processi interni all'azienda relativi ai due applicativi in esame ed abbiamo verificato che non ci fossero dei rischi che non sono stati presi in considerazione dall'azienda, e la fase di Test of Design dove si analizza il Design of Control, ovvero se la procedura di controllo descritta dall'azienda sia effettivamente efficace nella mitigazione dei rischi per cui è preposta. Questo si può fare attraverso le evidenze che ci sono state fornite al termine della riunione con i referenti IT della Società per ogni controllo. Quindi per ogni processo che ci è stato introdotto nella fase precedente (creazione utenza, password policy, separazione ambienti, backup, ecc.) abbiamo ottenuto le evidenze

richieste e verificato passo per passo l'esecuzione della procedura per capire che i rischi fossero effettivamente mitigati dai procedimenti effettuati. Questa fase serve per capire sostanzialmente 2 cose:

- Che il controllo indirizzi correttamente i rischi identificati;
- Che il controllo funzioni effettivamente come ci è stato spiegato in fase di understanding.

Di seguito la riproduzione di alcuni WTT realizzati durante il progetto, opportunamente anonimizzati.

Modifica sull'applicativo:

Richiesta di Change – In data 24/01/2018 un dipendente richiede una modifica attraverso l'apertura del ticket "DMNDXXXX" sul servizio di ticketing. Come si può

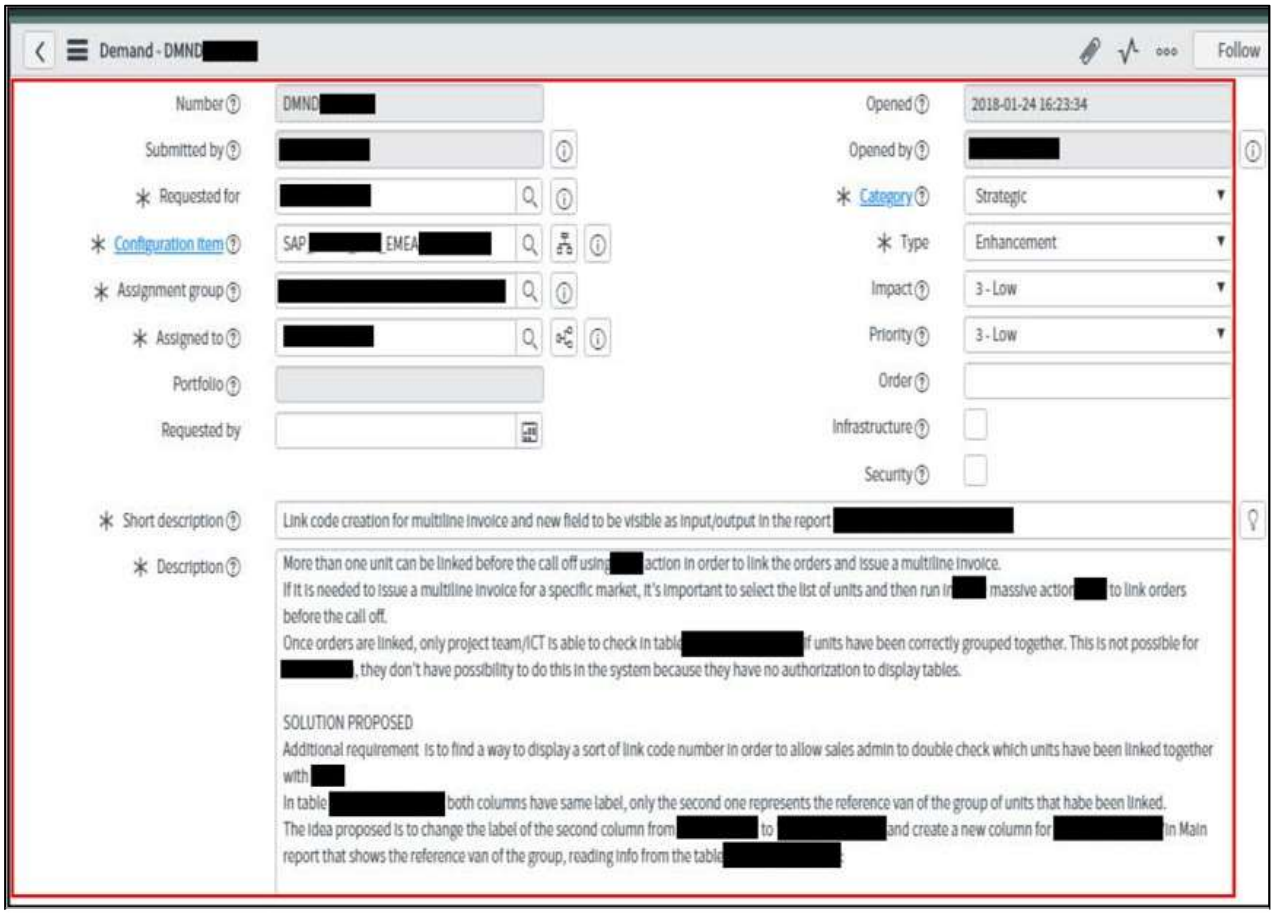


Figura 2: richiesta di change attraverso servizio di ticketing

notare dalla **figura 2** l'utente di business richiede una modifica dei campi visualizzabili in un determinato report sull'applicativo. La modifica ha un impatto sull'applicativo e una priorità classificati come "low", quindi la modifica non porta cambiamenti particolarmente rilevanti all'applicativo e inoltre non è urgente, infatti, come si potrà osservare in seguito questa modifica è stata trasportata in ambiente di produzione in data 17/03/2019, ovvero più di un anno dopo la sua richiesta.

Approvazione dello sviluppo - In seguito alla richiesta dell'utente di Business, due persone abilitate approvano lo sviluppo della Change e viene creato sullo strumento di ticketing un processo per seguire la fase di sviluppo e di test.

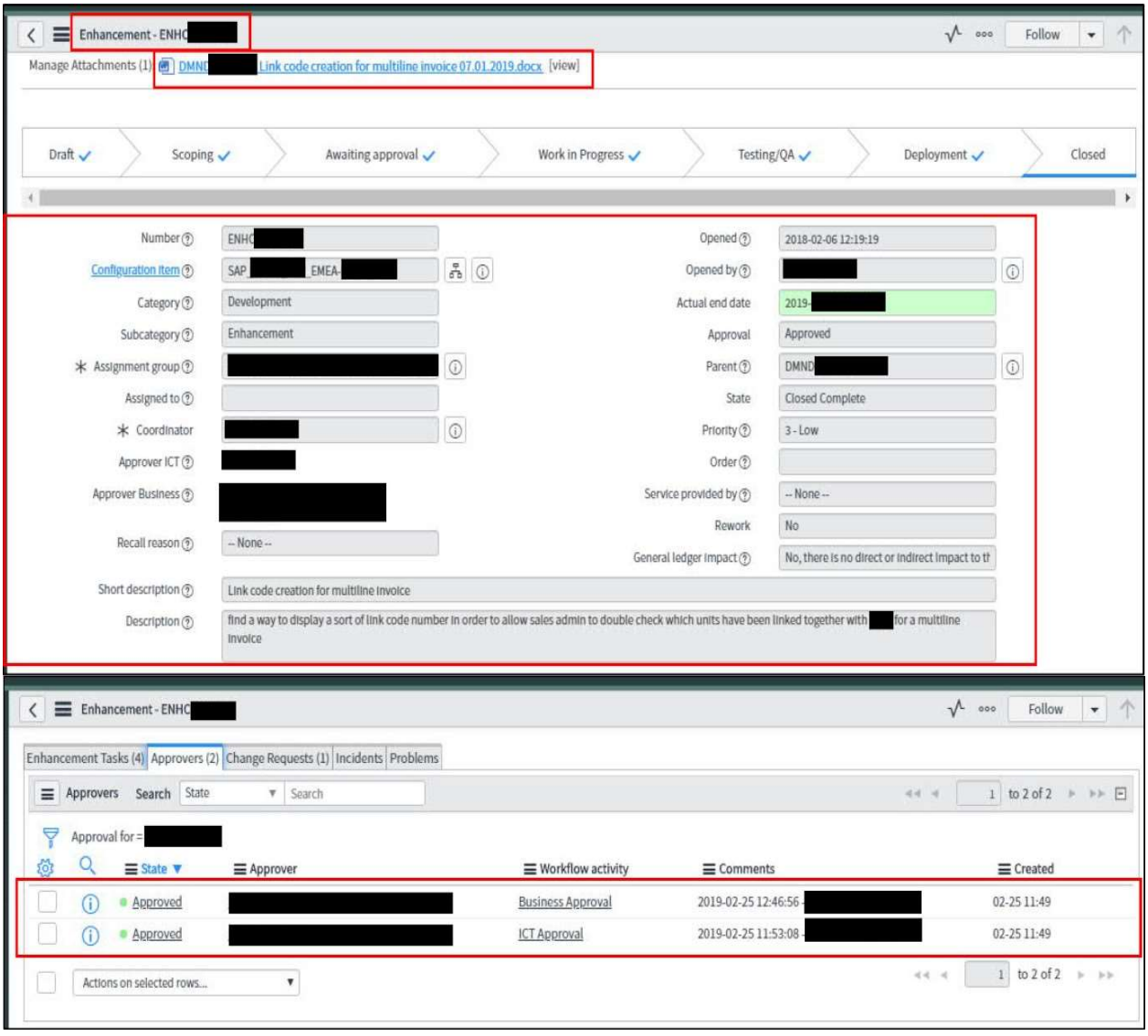


Figura 3: Approvazione della modifica

Sviluppo e fase di test – La modifica è sviluppata da una società esterna che collabora per contratto con l'azienda X. Una volta terminato lo sviluppo il richiedente effettua il test UAT per verificare che le sue richieste siano state soddisfatte e provvede a comunicarne i risultati (in questo caso positivi) tramite mail.

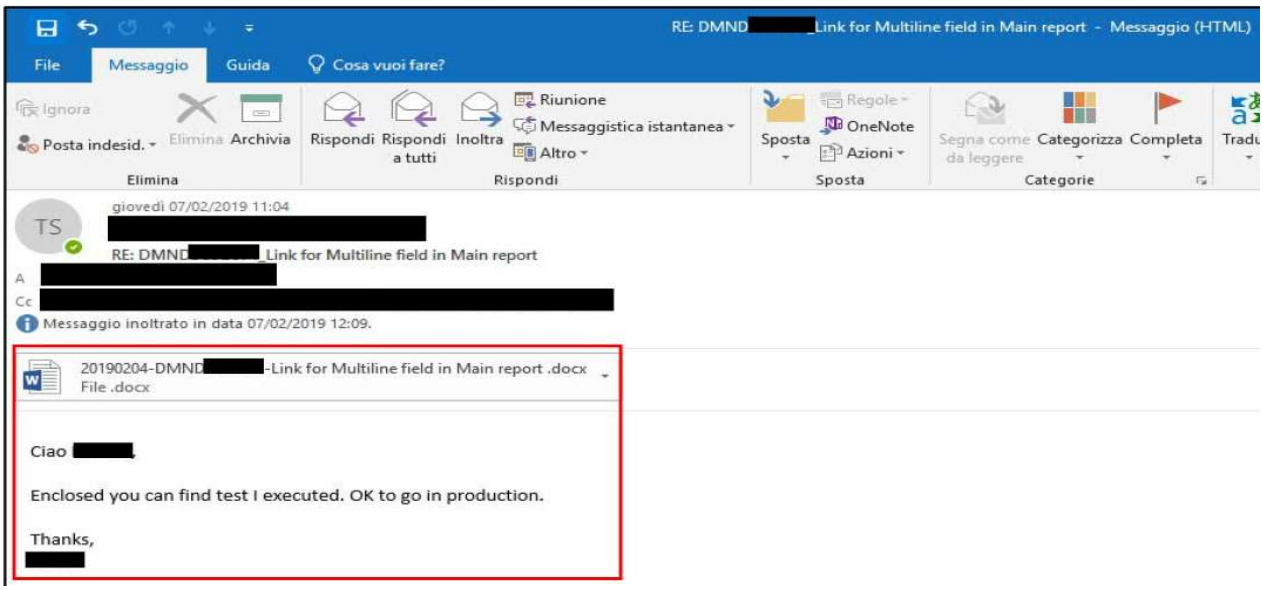


Figura 4: Esito del test UAT

Passaggio in produzione – Una volta superato l'UAT viene autorizzato il passaggio in produzione della modifica. Trasportata i produzione la modifica è considerata conclusa.

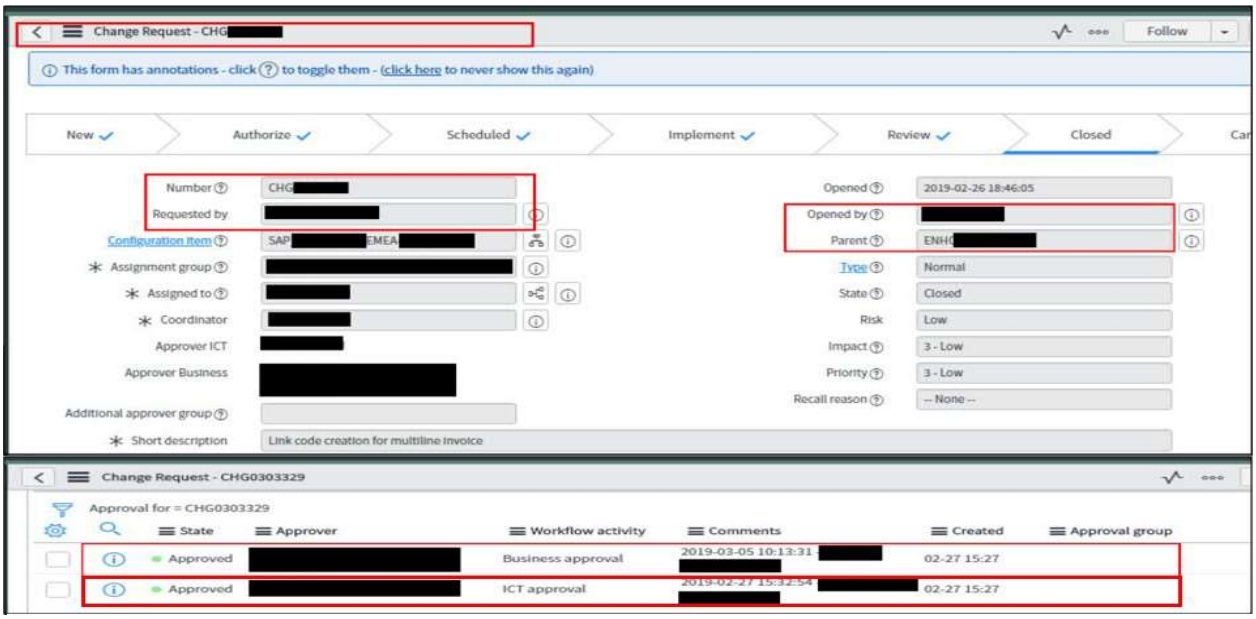
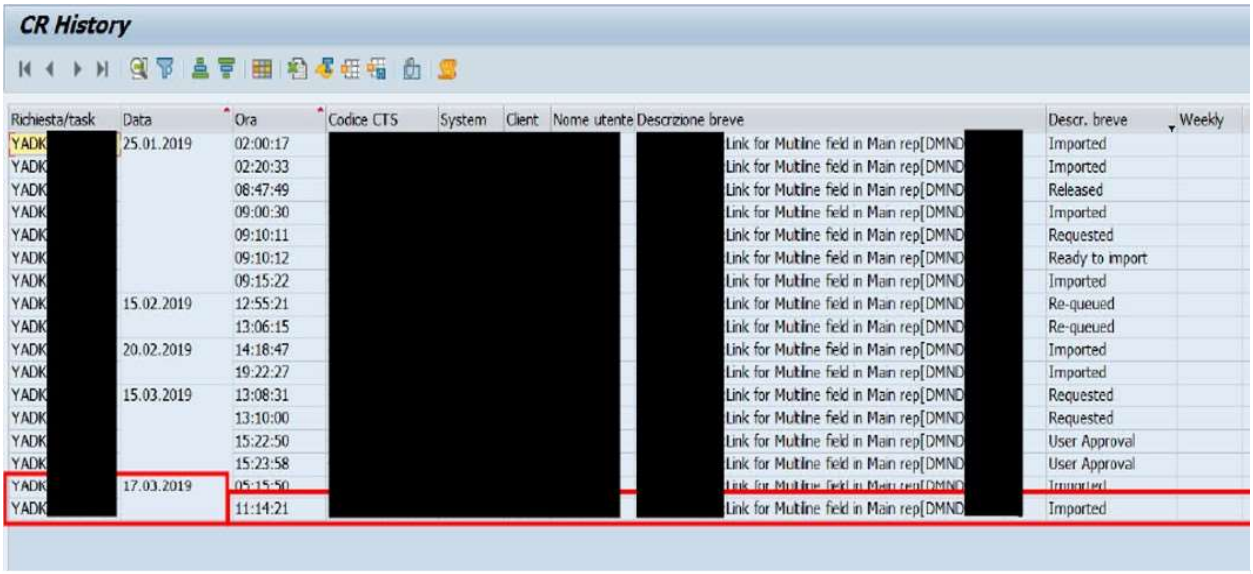


Figura 5: approvazione al trasporto in produzione

Effettiva installazione della modifica – Terminato il passaggio in produzione viene informato il richiedente della change con la "transport request". Nel caso specifico la modifica è stata importata il giorno 17/03/2019.



CR History

Richiesta/task	Data	Ora	Codice CTS	System	Client	Nome utente	Descrizione breve	Descr. breve	Weekly
YADK[redacted]	25.01.2019	02:00:17	[redacted]				Link for Mutline field in Main rep[DMND[redacted]	Imported	
YADK		02:20:33					Link for Mutline field in Main rep[DMND	Imported	
YADK		08:47:49					Link for Mutline field in Main rep[DMND	Released	
YADK		09:00:30					Link for Mutline field in Main rep[DMND	Imported	
YADK		09:10:11					Link for Mutline field in Main rep[DMND	Requested	
YADK		09:10:12					Link for Mutline field in Main rep[DMND	Ready to import	
YADK		09:15:22					Link for Mutline field in Main rep[DMND	Imported	
YADK	15.02.2019	12:55:21					Link for Mutline field in Main rep[DMND	Re-queued	
YADK		13:06:15					Link for Mutline field in Main rep[DMND	Re-queued	
YADK	20.02.2019	14:18:47					Link for Mutline field in Main rep[DMND	Imported	
YADK		19:22:27					Link for Mutline field in Main rep[DMND	Imported	
YADK	15.03.2019	13:08:31					Link for Mutline field in Main rep[DMND	Requested	
YADK		13:10:00					Link for Mutline field in Main rep[DMND	Requested	
YADK		15:22:50					Link for Mutline field in Main rep[DMND	User Approval	
YADK		15:23:58					Link for Mutline field in Main rep[DMND	User Approval	
YADK	17.03.2019	05:15:50					Link for Mutline field in Main rep[DMND	Imported	
YADK		11:14:21					Link for Mutline field in Main rep[DMND	Imported	

Figura 6: Transport Request della modifica in esame

Segregazione degli ambienti

Il test sulla segregazione degli ambienti è "one-shot", ovvero si effettua una sola volta l'anno, e consiste nel farsi fornire dall'azienda revisionata l'evidenza della presenza di più ambienti sull'applicativo in scopo. Di seguito la prova della presenza di tre ambienti (sviluppo, test e produzione) per l'applicativo SAP della società X.

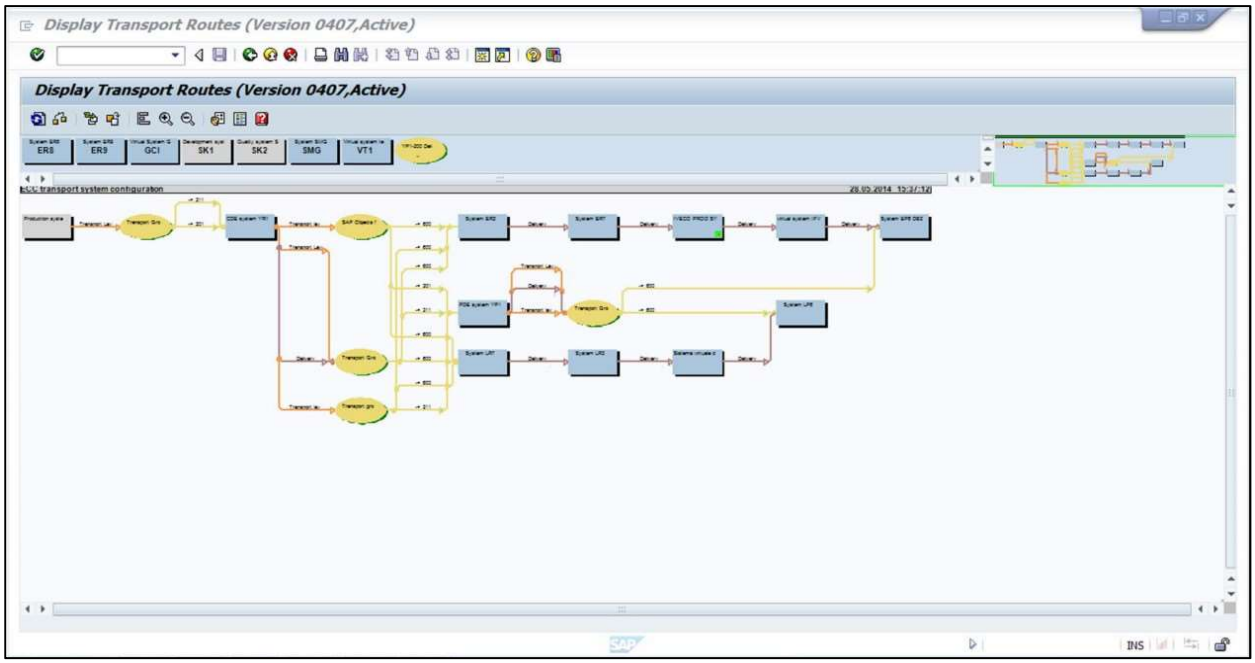


Figura 7: separazione ambienti su SAP

Creazione di una nuova utenza

Richiesta creazione utenza – In data 21/06/2019 è richiesta la creazione di una nuova utenza sull'applicativo SAP, attraverso il sistema di ticketing, da parte di un utente del dipartimento IT.

Ticket number	SAP[redacted]
Request date	2019-06-21T10:12:29

Hide info

Requester Data			
UserID	[redacted]	Domain	[redacted]
Last Name	[redacted]	First Name	[redacted]
E-mail	[redacted]@[redacted].com	Telephone	
Company	[redacted]	Address	[redacted]
Country	Italy	Department	[redacted]INFORMATION & COMM TECHNOLOGY
Location	TO	Job function	

End user Data			
UserID	[redacted]	Domain	[redacted]
Last Name	[redacted]	First Name	[redacted]
E-mail	[redacted]@[redacted].com	Telephone	
Company	[redacted]	Address	[redacted]
Country	Italy	Department	[redacted] INFORMATION & COMM TECHNOLOGY
Location	TO	Job function	
User type	consultant		

Figura 8: Richiesta creazione utenza PT1

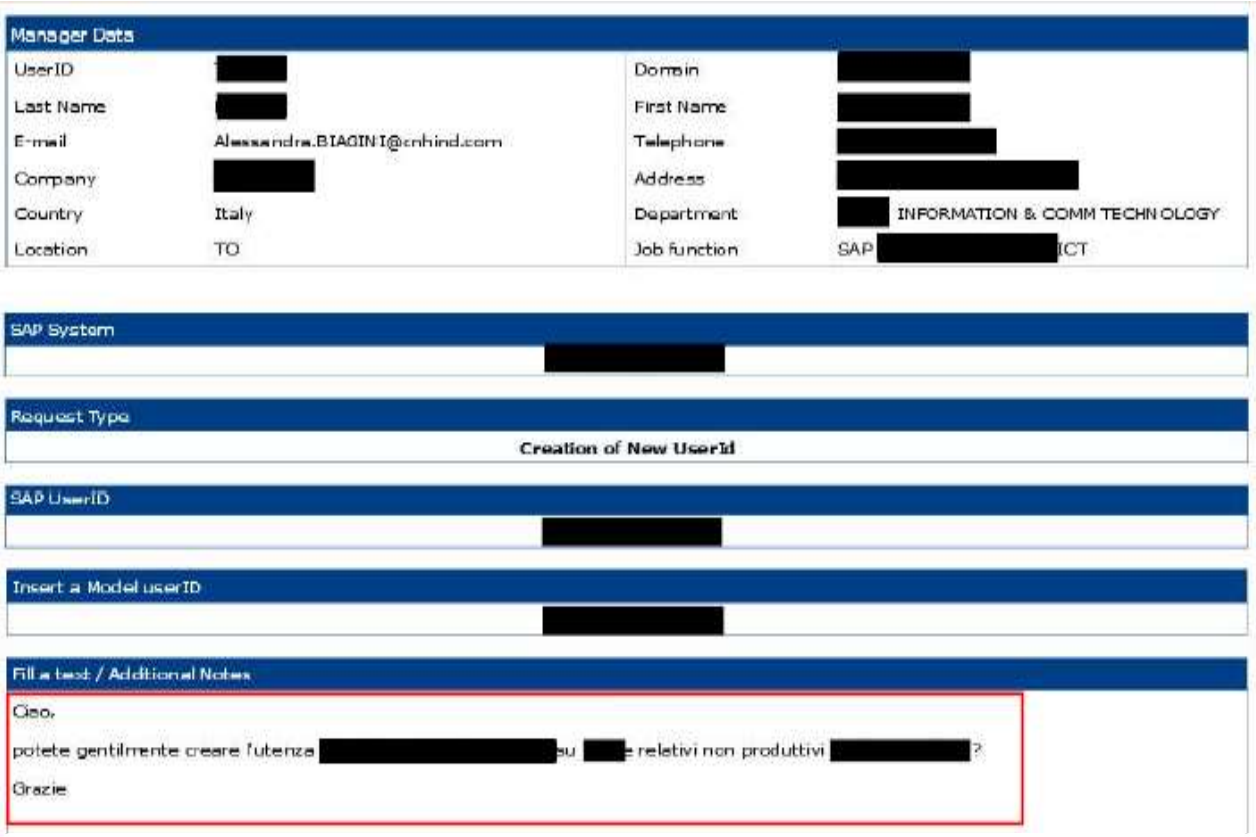


Figura 9: richiesta creazione utenza PT2

Approvazione della creazione – Il Manager approva la creazione della nuova utenza sull'applicativo.

Figura 10: approvazione da parte del personale appropriato

Creazione dell'utenza e chiusura del ticket – Una volta approvata l'utenza viene creata, in data 26/06/2019. In seguito alla creazione vengono comunicati tramite mail i dati d'accesso e il ticket viene chiuso dal personale che ha provveduto a creare l'utenza.

User ID	[redacted]	**Display Name**	[redacted]
Activity	Request Sent	**Action**	Request Sent
Note		**Date**	06/21/2019 10:16:20

User ID	[redacted]	**Display Name**	[redacted]
Activity	In Charge to Security (1 Level)	**Action**	Validate by [redacted]
Note	Sent to [redacted] for approval.	**Date**	06/26/2019 12:46:25

User ID	[redacted]	**Display Name**	[redacted]
Activity	Business Approval (1 level)	**Action**	Task completed
Note		**Date**	06/26/2019 13:06:03

User ID	[redacted]	**Display Name**	[redacted]
Activity	In Charge to Security (2 Level)	**Action**	Task completed
Note	User has been created in all Systems. Regards, [redacted]	**Date**	06/26/2019 14:22:36

User ID	[redacted]	**Display Name**	[redacted]
Activity	Completed - EndUser Check	**Action**	Completed - EndUser Check Task expired
Note		**Date**	07/01/2019 14:22:42

Figura 11: chiusura del ticket

Job

Verifica della corretta esecuzione – Per il controllo dei job è necessario verificare che questi ultimi siano completati correttamente, di conseguenza è stata presa come riferimento la settimana dal 25/10/2019 al 30/10/2019 per uno dei 10 job programmati per effettuare l'analisi

Come si può vedere dall'immagine gli esiti, per il periodo in questione, gli esiti sono tutti positivi.

Data	Descrizione
05:55:01 25.10.2019	BATCHMAN:+ AWS[redacted] Job[redacted](0600 10/24/19),(0AAAAAAAAABL7WU)].DOC1_[redacted] UNTIL time 5:55 has occurred. The UNTIL user option is SUPPRESS
05:55:01 25.10.2019	BATCHMAN:AWS[redacted] Job stream[redacted](0600 10/24/19),(0AAAAAAAAABL7WU)] has completed successfully.
05:55:01 25.10.2019	BATCHMAN:AWS[redacted] Changing job stream[redacted](0600 10/24/19),(0AAAAAAAAABL7WU)] status to SUCC.
05:55:01 26.10.2019	BATCHMAN:+ AWS[redacted] Job[redacted](0600 10/25/19),(0AAAAAAAAABMAQK)].DOC1_[redacted] UNTIL time 5:55 has occurred. The UNTIL user option is SUPPRESS
05:55:01 26.10.2019	BATCHMAN:AWS[redacted] Job stream[redacted](0600 10/25/19),(0AAAAAAAAABMAQK)] has completed successfully.
05:55:01 26.10.2019	BATCHMAN:AWS[redacted] Changing job stream[redacted](0600 10/25/19),(0AAAAAAAAABMAQK)] status to SUCC.
05:55:02 27.10.2019	BATCHMAN:+ AWS[redacted] Job[redacted](0600 10/26/19),(0AAAAAAAAABMAQL)].DOC1_[redacted] UNTIL time 5:55 has occurred. The UNTIL user option is SUPPRESS
05:55:02 27.10.2019	BATCHMAN:AWS[redacted] Job stream[redacted](0600 10/26/19),(0AAAAAAAAABMAQL)] has completed successfully.
05:55:02 27.10.2019	BATCHMAN:AWS[redacted] Changing job stream[redacted](0600 10/26/19),(0AAAAAAAAABMAQL)] status to SUCC.
05:55:02 28.10.2019	BATCHMAN:+ AWS[redacted] Job[redacted](0600 10/27/19),(0AAAAAAAAABMAQM)].DOC1_[redacted] UNTIL time 5:55 has occurred. The UNTIL user option is SUPPRESS
05:55:02 28.10.2019	BATCHMAN:AWS[redacted] Job stream[redacted](0600 10/27/19),(0AAAAAAAAABMAQM)] has completed successfully.
05:55:02 28.10.2019	BATCHMAN:AWS[redacted] Changing job stream[redacted](0600 10/27/19),(0AAAAAAAAABMAQM)] status to SUCC.
05:55:02 29.10.2019	BATCHMAN:+ AWS[redacted] Job[redacted](0600 10/28/19),(0AAAAAAAAABMAQN)].DOC1_[redacted] UNTIL time 5:55 has occurred. The UNTIL user option is SUPPRESS
05:55:02 29.10.2019	BATCHMAN:AWS[redacted] Job stream[redacted](0600 10/28/19),(0AAAAAAAAABMAQN)] has completed successfully.
05:55:02 29.10.2019	BATCHMAN:AWS[redacted] Changing job stream[redacted](0600 10/28/19),(0AAAAAAAAABMAQN)] status to SUCC.
05:55:02 30.10.2019	BATCHMAN:+ AWS[redacted] Job[redacted](0600 10/29/19),(0AAAAAAAAABMAQO)].DOC1_[redacted] UNTIL time 5:55 has occurred. The UNTIL user option is SUPPRESS
05:55:02 30.10.2019	BATCHMAN:AWS[redacted] Job stream[redacted](0600 10/29/19),(0AAAAAAAAABMAQO)] has completed successfully.
05:55:02 30.10.2019	BATCHMAN:AWS[redacted] Changing job stream[redacted](0600 10/29/19),(0AAAAAAAAABMAQO)] status to SUCC.

Figura 12: dettaglio del job dal giorno 25/10/2019 al 30/10/2019

Backup

Verifica della corretta esecuzione – Di seguito viene presentato un esempio di backup offline terminato con successo in data 14/1/2109Il backup è iniziato il giorno 14/10/2019 ed è terminato con successo come mostrato nel log nella figura di seguito alle ore 06:11.

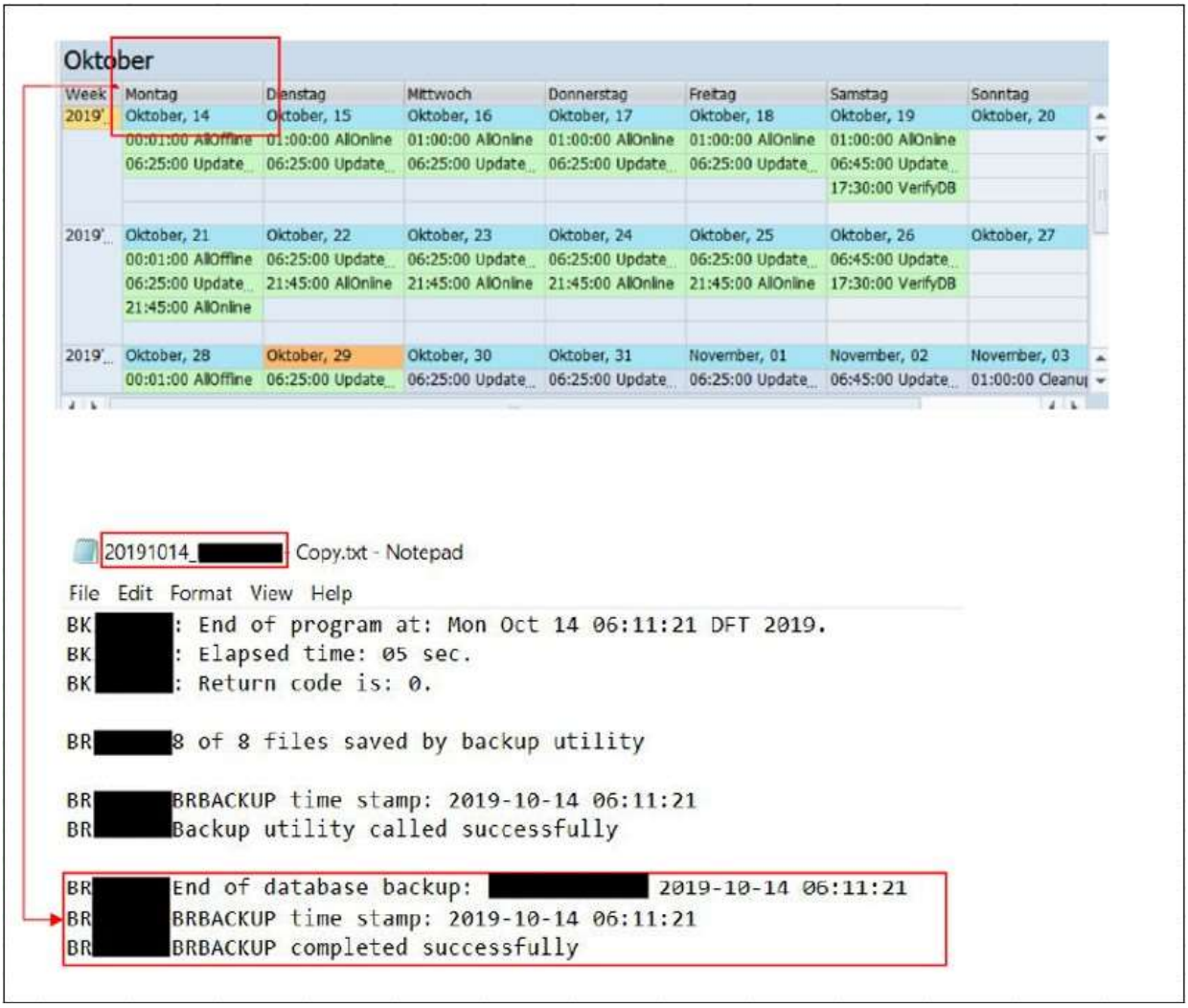


Figura 13: log del backup effettuato in data 14/10/2019

3.3.3 Test of Effectiveness

Una volta verificato, attraverso la fase di WTT, che i controlli mitighino effettivamente i rischi identificati è possibile passare alla fase successiva, ovvero quella dei test di efficacia. Questa fase è stata quella più lunga e impegnativa del progetto, poiché consiste nel testare dei campioni delle popolazioni di item dei vari controlli al fine di verificare che si comportino effettivamente secondo progetto, ovvero che seguano il design of control che l'azienda ci ha spiegato ed abbiamo confermato osservando le evidenze durante la fase di Test of Design. Per i controlli one-shot, quelli che sono effettuati una volta l'anno e di conseguenza la popolazione è soltanto di uno, non è stato necessario effettuare nuovamente il test, poiché è stato sufficiente rimandare ai

risultati osservati e redatti in WTT; invece per tutti gli altri controlli abbiamo dovuto richiedere ai referenti IT dei due applicativi le popolazioni dei processi al fine di effettuare il campionamento. Le popolazioni di item solitamente consistono in estrazioni di report dall'applicativo ad Excel, nelle quali sono indicati tutti gli item relativi a un determinato processo, con eventuali date e codici identificativi. Ad esempio, per le modifiche effettuate sull'applicativo SAP, la popolazione consiste nell'esportazione su Excel della tabella "E070", ovvero un registro nel quale sono elencate tutte le modifiche che sono state trasportate in produzione in un determinato periodo (nel nostro caso un anno, l'analisi andava dal 01/01/2019 al 31/12/2019). Insieme alla popolazione la metodologia prevede che ci si faccia fornire evidenze di completezza, ovvero degli elementi che hanno lo scopo di provare che la popolazione di item che ci è stata trasmessa non sia stata manomessa e contenga effettivamente tutti gli itemrelativa al periodo di audit. Solitamente la completeness consiste in un screenshot della richiesta di estrazione che contenga sia il numero di righe della tabella sia la data del giorno in cui è stata effettuata; il nostro compito è di verificare che il numero di righe indicate nell'evidenza di completezza corrisponda al numero della popolazione su Excel (in **figura 14** è rappresentata la completeness dell'estrazione di una tabella E070 di SAP).

Ottenute le popolazioni dei vari processi abbiamo effettuato il campionamento con un software interno all'azienda che permette di selezionare casualmente una serie di elementi da una popolazione. È infatti fondamentale che gli item siano selezionati randomicamente per poter trarre conclusioni statisticamente affidabili sull'intera popolazione. La dimensione del campione corrisponde al 10% della popolazione totale con un minimo di 5 (a meno che la popolazione non sia inferiore alle 5 unità, in quel caso si prenderà l'intera popolazione) ad un massimo di 25.

Una volta effettuati i campioni per tutti i controlli da testare, il passo successivo è stato quello di richiedere ai referenti le evidenze per poter effettuare i test sugli item selezionati.

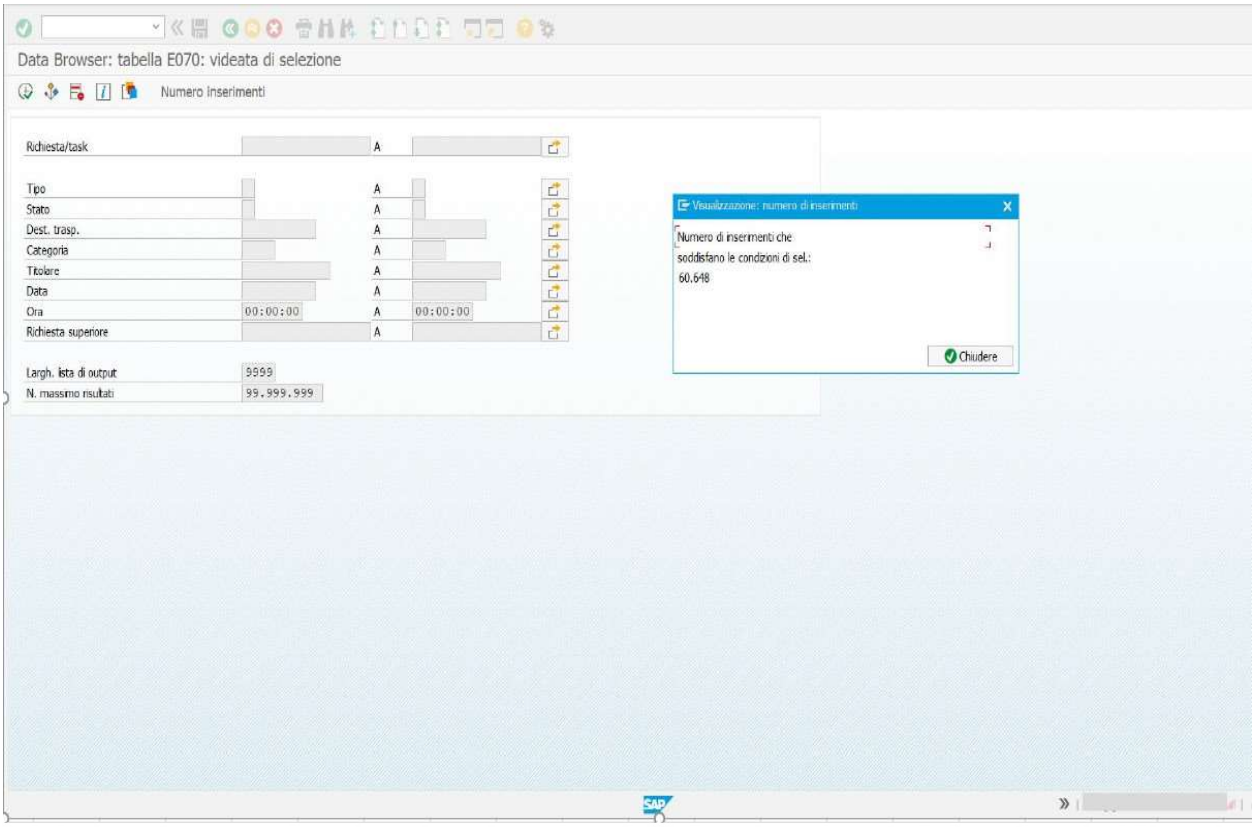


Figura 14: evidenza di completeness dell'estrazione di una tabella E070

Questa fase del processo di audit richiede tempi lunghi per vari motivi, sia perché è necessario del tempo per formalizzare i test dei controlli, specialmente quando ci sono campioni grandi, il che è piuttosto comune, sia perché i tempi di raccolta dei documenti da parte del personale del cliente non sono brevi. In particolare con l'azienda X i tempi di raccolta del materiale sono stati lunghi prevalentemente per due motivi: in primis a causa delle difficoltà per accedere all'ufficio a causa dell'emergenza sanitaria; in secondo luogo perché l'azienda in questione si è sottoposta al processo di audit volontariamente, ed essendo uno dei primi anni in cui era effettuata la revisione dei sistemi informativi, i dipendenti non avevano un processo ben strutturato in grado di rispondere rapidamente alla nostre richieste, di conseguenza alcune volte non sapevano dove reperire il materiale da mandarci e questo ha causato l'allungamento dei tempi di attesa.

Ottenute le evidenze abbiamo proceduto con la formalizzazione degli ITGC. La formalizzazione avviene su dei documenti di excel che contengono varie informazioni sul controllo. Sul primo foglio vi sono una serie di informazioni riguardo al test effettuato (nome dell'azienda, descrizione dei controlli testati, processo di riferimento, finestra di audit) e la conclusione sull'effettiva efficacia o inefficacia del controllo. Nei fogli successivi al primo vi è la formalizzazione del test con le evidenze ricevute dal referente, in ogni foglio è formalizzato un item.

In **figura 15** è mostrata la tabella riassuntiva che abbiamo costruito per la selezione del campione del test sulle change dell'applicativo SAP. Come si può notare sono elencate la popolazione di item, la dimensione del campione e il metodo con cui è stato estratto il campione. Nel file allegato sono presenti le evidenze di completezza della popolazione e le schermate del programma per la selezione del campione per provare effettivamente che il campione testato sia quello estratto dal programma.

Campione del Test Of Control

Fonte della popolazione	SAP
Dimensione della popolazione	1563
Dimensione del campione	25
Procedure per determinare la completezza	Campione Modifiche SAP
Metodo di selezione	Programma per estrazione dei campioni di EY

Figura 15: riassunto della selezione del campione

In **figura 16** è presente la tabella riassuntiva del test sulle modifiche all'applicativo, nella quale sono elencati gli item campionati e per ogni elemento del campione è indicato: il codice univoco di riferimento (nel caso di SAP è il codice univoco che viene associato sul sistema ad ogni singola modifica trasportata), la data di approvazione della modifica, quella di test e quella del trasporto in produzione, come si può notare la terza è sempre successiva alla seconda e la seconda alla prima, altrimenti il controllo, dopo opportune verifiche con i responsabili IT dell'applicativo, sarebbe stato dichiarato ineffective. Sulla parte destra della tabella vi sono i controlli sui singoli attributi, specificati sotto la tabella principale.

Procedura di Test

								MC1.3			
Item testato	**Codice**	**Data approvazione modifica**	**Data test**	**Data passaggio in produzione**	**Test**	**Approvazione**	**Trasporto**	**A**	**B**	**C**	**D**
29	SK[redacted]	08/08/2019	10/08/2019	10/08/2019	[redacted]			X	X	X	X
105	SK[redacted]	10/05/2019	13/05/2019	15/05/2019				X	X	X	X
189	SK[redacted]	22/05/2019	23/05/2019	24/05/2019				X	X	X	X
245	SK[redacted]	22/08/2019	23/08/2019	23/08/2019				X	X	X	X
254	SK[redacted]	14/08/2019	17/08/2019	17/08/2019				X	X	X	X
306	SK[redacted]	20/12/2019	20/12/2019	21/12/2019				X	X	X	X
392	SK[redacted]	12/03/2019	13/03/2019	13/03/2019				X	X	X	X
472	SK[redacted]	13/09/2019	14/09/2019	14/09/2019				X	X	X	X
481	SK[redacted]	28/04/2019	28/04/2019	30/04/2019				X	X	X	X
494	SK[redacted]	11/11/2019	11/11/2019	13/11/2019				X	X	X	X
516	SK[redacted]	21/02/2019	21/02/2019	23/02/2019				X	X	X	X
542	SK[redacted]	17/08/2019	20/08/2019	23/08/2019				X	X	X	X
576	SK[redacted]	27/07/2019	02/07/2019	03/08/2019				X	X	X	X
580	SK[redacted]	10/02/2019	13/02/2019	14/02/2019				X	X	X	X
582	SK[redacted]	22/01/2019	24/01/2019	25/01/2019				X	X	X	X
694	SK[redacted]	07/06/2019	07/06/2019	08/06/2019				X	X	X	X
919	SK[redacted]	06/06/2019	10/06/2019	10/06/2019				X	X	X	X

Attributes MC1.3 - Changes to application configurations are adequately tested and approved before being migrated into production.	
A	EY inspected that the configuration change was tested.
B	EY inspected that configuration change was approved by appropriate Company Responsible.
C	EY inspected that the configuration change was moved into production following to the approval.
D	EY inspected that the personnel who developed the configuration change is different from the personnel involved in moving the change

Note	
X	L'attributo è soddisfatto

Figura 16: tabella riassuntiva del test del controllo.

Infine, in **figura 17** è raffigurata la tabella conclusiva nel quale viene indicato l'esito del test sul controllo e la presenza o meno di eccezioni, che in questo caso non c'erano. Se si presentassero delle anomalie durante la fase di test dovrebbe essere messa la spunta "Si" in questa tabella, e in quel caso si aggiungerebbe una casella nella quale avremmo scritto quali sono le eccezioni incontrate, quali spiegazioni sono state fornite in merito

dai referenti IT della società e se tali anomalie sono sufficienti per rendere il controllo ineffective oppure no.

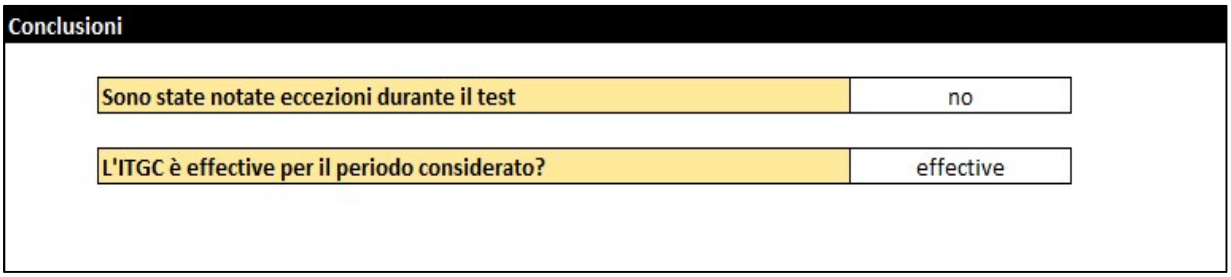


Figura 17: conclusioni sul test effettuato

Nel caso di un controllo diverso, ad esempio sui backup o sulla creazione utenze, il report prodotto è circa lo stesso (con le ovvie modifiche alle colonne della tabella); l'unica vera differenza sarebbero gli attributi dei controlli, che sono strettamente legati al controllo in essere.

Il documento rappresentato in tabella è una riproduzione degli aspetti salienti di quello utilizzato dall'azienda per la formalizzazione dei test sui controlli ITGC, poiché, per ragioni di segretezza aziendale non mi è permesso riportare all'esterno dell'azienda il file originale. Inoltre, anche il nome del software per effettuare il campionamento non è stato riportato per le stesse ragioni.

Durante questa fase di test delle modifiche all'applicativo SAP è successo che abbiamo dovuto effettuare un ricampionamento di alcune change campionate, poiché, nonostante risultassero dalla tabella E070 come modifiche all'applicativo, di fatto si sono rivelati essere soltanto delle aperture di ticket a seguito di rallentamenti del sistema, che di fatto si sono risolti da soli senza che qualcuno dovesse effettuare nessuna modifica, di conseguenza non potevano essere formalizzati come test sulle change e quindi abbiamo dovuto effettuare un ulteriore campionamento per ottenere nuovi item. Questo fatto ha ulteriormente rallentato questa fase, poiché abbiamo dovuto attendere che i referenti ci inviassero le nuove evidenze.

La fase di test degli ITGC termina quando sono stati effettuati i test su tutti i controlli relativi ai processi di MA, MC e MO.

3.3.4 Individuazione e test degli ITAC

Gli ITAC sono controlli effettuati su delle componenti automatiche implementate negli applicativi in scopo, ovvero l'azienda ha inserito all'interno dell'applicativo dei processi che sono svolti in completa autonomia, un classico esempio è la creazione delle fatture. Ogni volta che c'è un'operazione completamente automatizzata vi deve essere un ITAC, ovvero un controllo che verifichi che quell'operazione funzioni correttamente. Gli ITAC, a differenza degli ITGC che ci sono stati presentati dai referenti della società cliente, non ci vengono introdotti da personale interno alla società, ma sono individuati dai revisori contabili che in seguito ci hanno passo direttive su cosa analizzare. Più precisamente i colleghi hanno identificato una parte del processo di manipolazione di dati contabili che fosse gestita interamente in maniera automatica sull'applicativo in esame e ci hanno chiesto di indagare in maniera più approfondita per capire se vi fosse effettivamente un ITAC e di conseguenza se avessimo dovuto testarlo, oppure no. Quindi abbiamo dovuto fare un altro meeting con un'altra persona della società X che ci è stata indicata come referente per questo processo. Durante questo incontro abbiamo osservato l'esecuzione del processo e siamo giunti a conclusione era effettivamente un processo completamente automatico controllato attraverso un ITAC. Quindi abbiamo fissato un altro incontro, sempre attraverso mezzi telematici, per poter effettuare il test sul controllo automatico. I test sugli ITAC sono svolti in maniera differente rispetto a quelli sugli ITGC, infatti, essendo automatico, il controllo dovrebbe funzionare sempre allo stesso modo, quindi non è prevista la fase di WTT, ma soltanto quella vera e propria di test, nella quale, per ovvi motivi, non viene effettuato un campione, ma sono verificati tutti gli scenari che si possono incontrare per appurare che il controllo funzioni correttamente, ovvero bloccando le azioni che non possono essere eseguite (negative test) e terminando le azioni che possono essere realizzate (positive test). Generalmente la fase di test degli ITAC è più rapida di quella degli ITGC, poiché vi è da formalizzare soltanto un numero limitato di scenari, rispetto alla formalizzazione dei campioni degli ITGC. Di seguito la formalizzazione dell'ITAC del processo di creazione delle fatture inserito nell'applicativo SAP dell'azienda X.

Generazione delle fatture:

- Attraverso la transazione VF04 vengono visualizzati tutti i documenti disponibili per la fatturazione.

Il risultato dell'estrazione mostra 5 risultati:

- doc. comm. 893001659; Nome Committente [redacted]
- doc. comm. 893001658; Nome Committente [redacted]
- doc. comm. 893001657; Nome Committente [redacted]
- doc. comm. 893001660; Nome Committente [redacted];
- doc. comm. 893001662; Nome Committente[redacted];

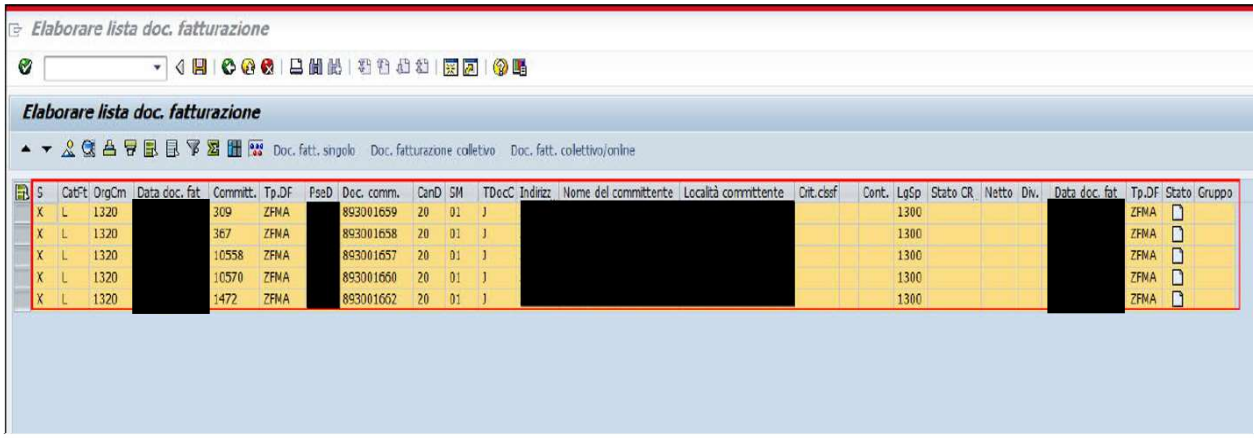


Figura 18: documenti disponibili per la fatturazione

- Mediante la transazione VFX3 il documento 993001132 (Nome Committente[redacted]), che si riferisce al doc. comm. 893001659, viene registrato in contabilità con successo.

Negli step di registrazione successivi, il documento viene sempre identificato dal campo "DocFatt" che indica il n° di protocollo e non la numerazione della fattura.

Nel processo di registrazione del documento non è mai presente un campo disponibile all'utente in cui inserire il numero di fattura.

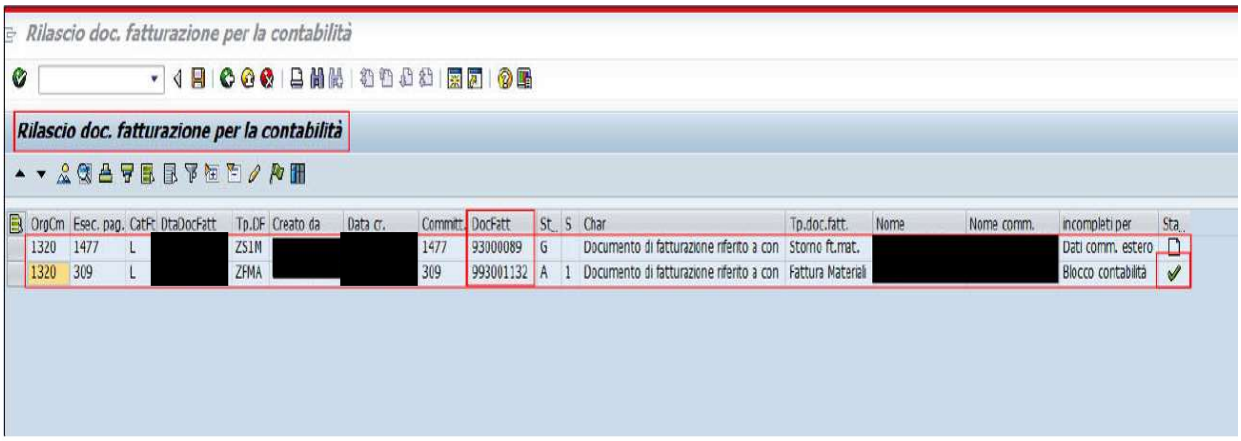


Figura 19: registrazione del documento in contabilità

- Mediante la transazione VF31 si procede con la generazione del documento PDF della fattura identificata dal n° di protocollo 993001132.

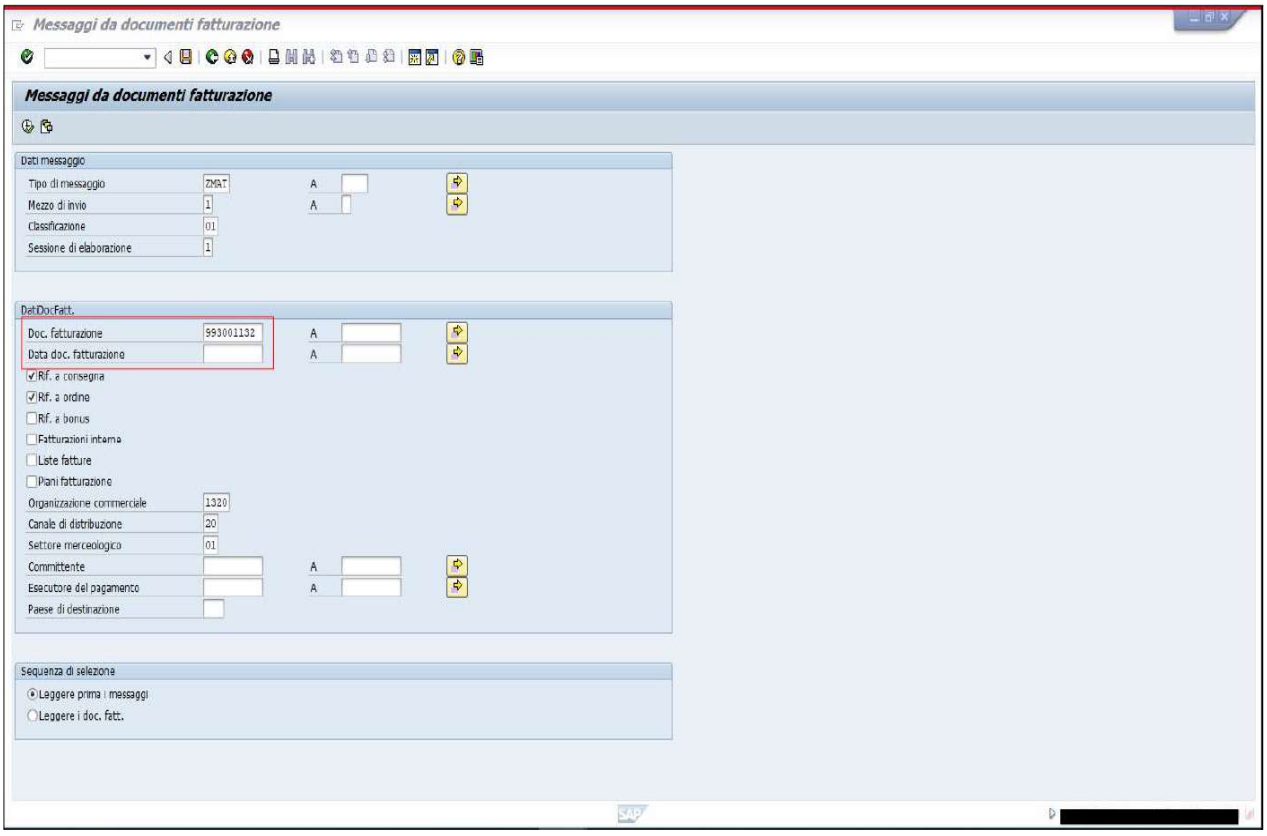


Figura 20: generazione del documento PDF

- In seguito, il sistema conferma l'avventua generazione con successo del PDF ed invia un messaggio di conferma.

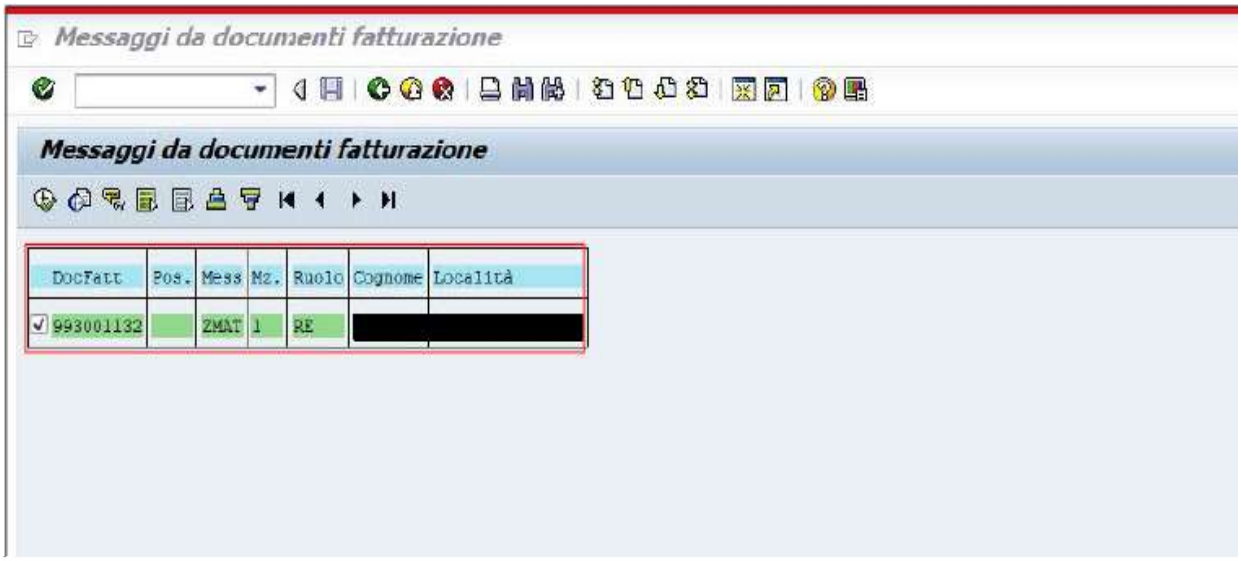


Figura 21: conferma avvenuta generazione del documento

- Creato il PDF, mediante la transazione ZPDF, viene richiesta la stampa del documento di fattura generato**.**

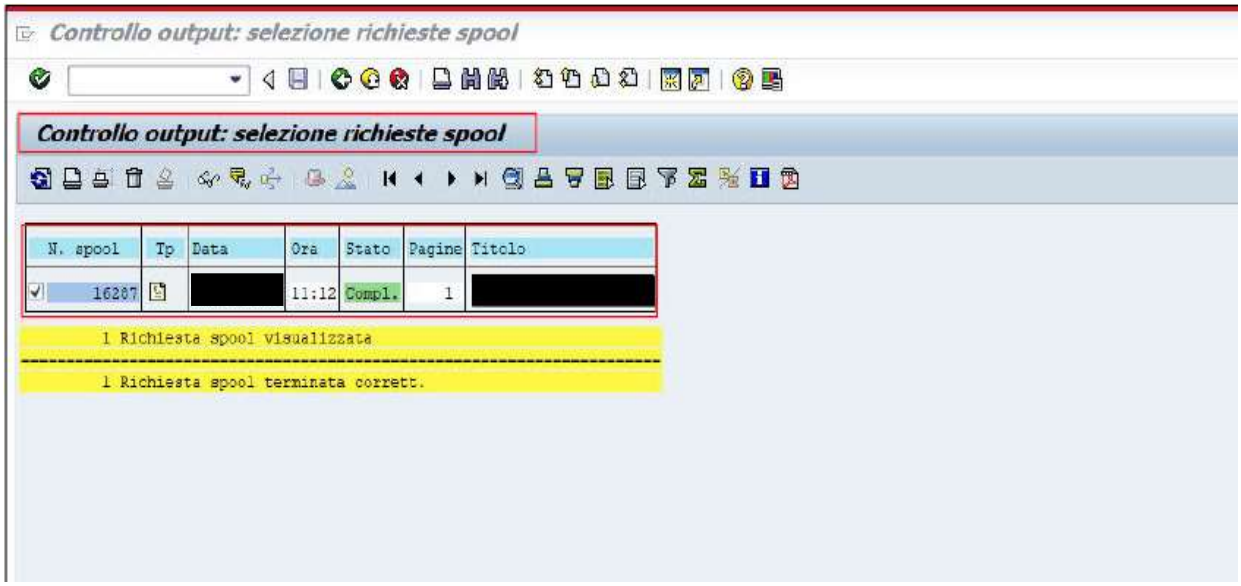


Figura 22: richiesta di stampa della fattura

- Il Numero di fattura viene generato automaticamente dal sistema SAP ed è visualizzabile solamente sul documento finale.

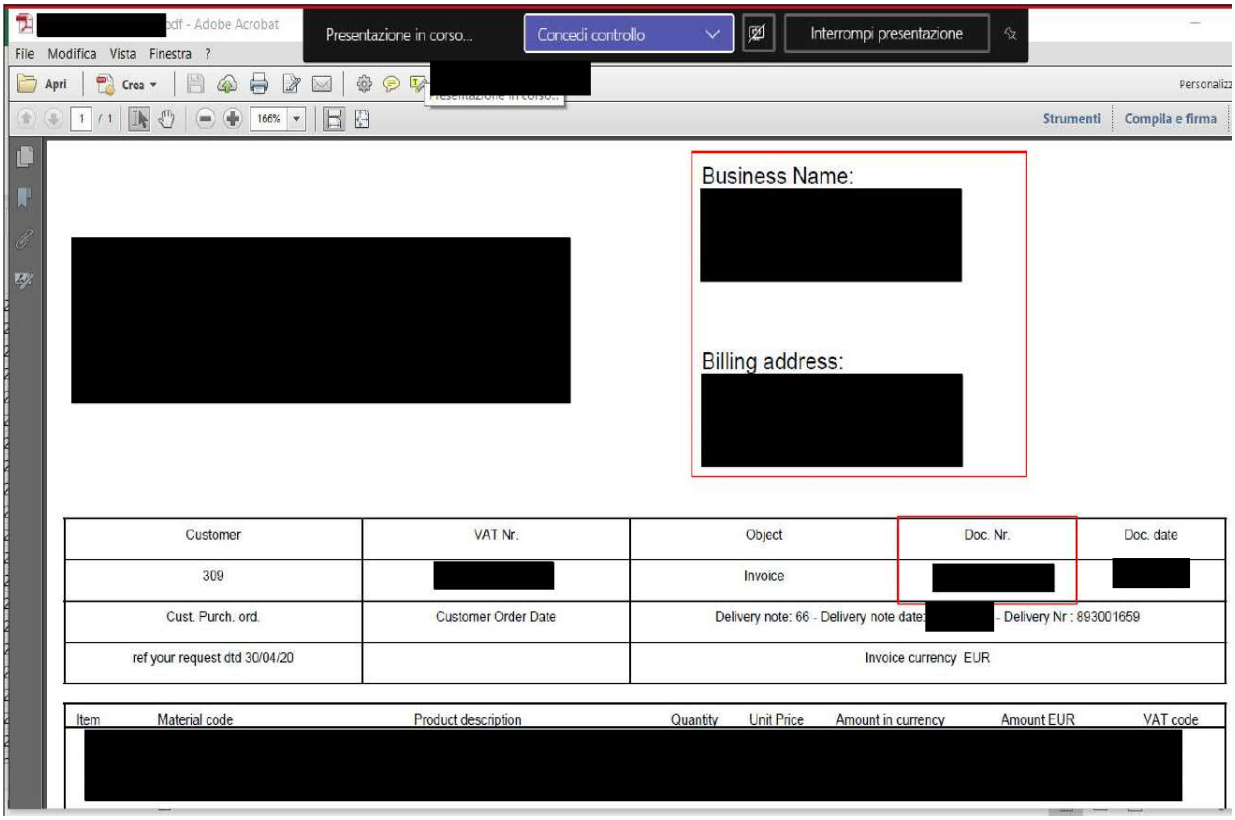


Figura 23: documento finale della fattura

Infine, la transazione FBL5N permette di visualizzare la lista partite singole debitorie, fra cui figura la fattura Numero [redacted] che corrisponde al n° di protocollo 993001132.

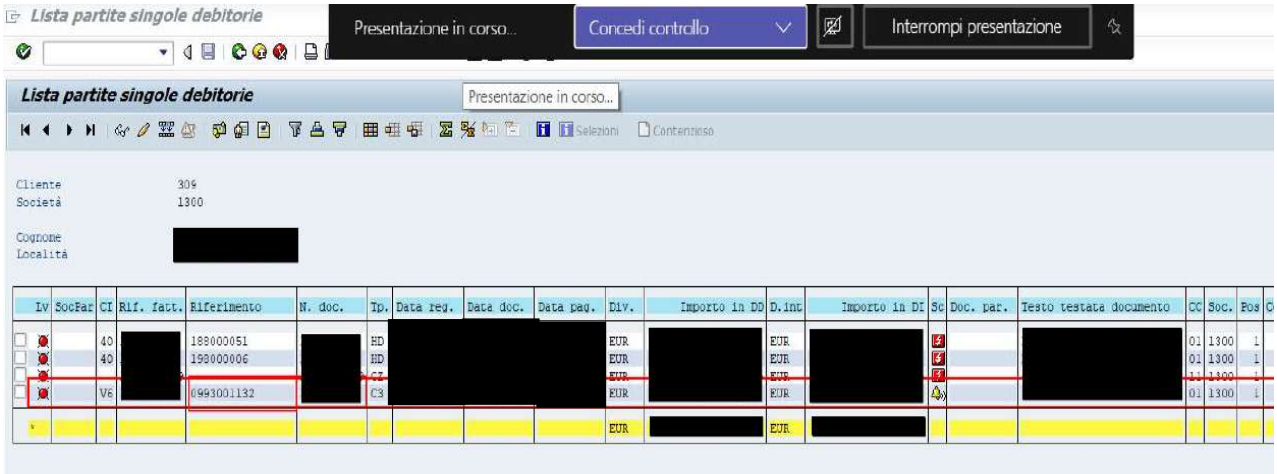
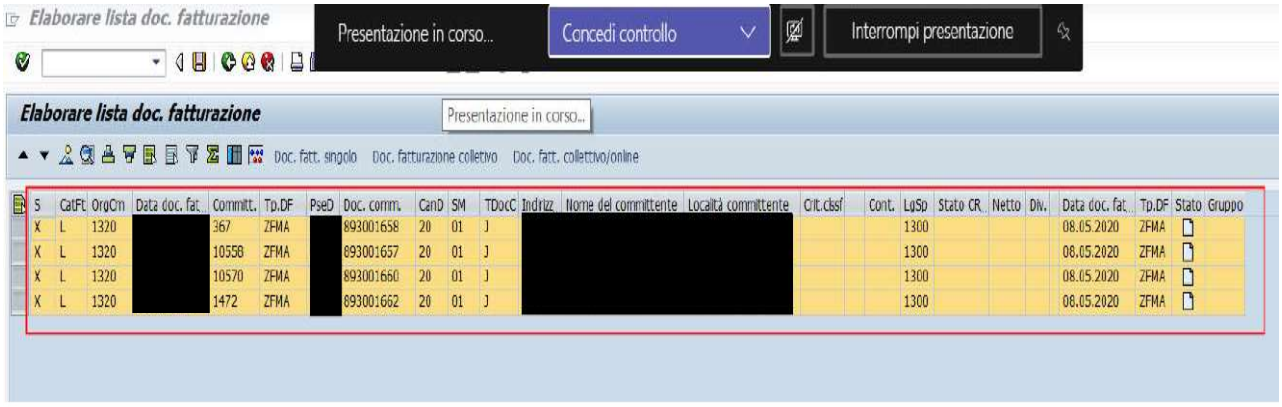


Figura 24: lista partite singole debitorie, in cui rientra la fattura appena generata

Eseguendo nuovamente la transazione VF04, al fine di visualizzare tutti i documenti disponibili per la fatturazione, il risultato dell'estrazione non mostra il documento 993001132 già registrato in contabilità.
Il sistema SAP, quindi, non permette la doppia emissione o la doppia numerazione di una stessa fattura.



S	CatFt	OrgCm	Data doc. fat.	Committ.	Tp.DF	PseD	Doc. comm.	CanD	SM	TDocC	Indriz.	Nome del committente	Località committente	Crit.class	Cont.	LgSp	Stato CR	Netto	Div.	Data doc. fat.	Tp.DF	Stato	Gruppo
X	L	1320	[redacted]	367	ZFMA	[redacted]	893001658	20	01	J	[redacted]					1300				08.05.2020	ZFMA		
X	L	1320		10558	ZFMA		893001657	20	01	J						1300				08.05.2020	ZFMA		
X	L	1320		10570	ZFMA		893001660	20	01	J						1300				08.05.2020	ZFMA		
X	L	1320		1472	ZFMA		893001662	20	01	J						1300				08.05.2020	ZFMA		

Figura 25: documenti disponibili alla fatturazione

Durante il controllo, come da descrizione del secondo capitolo, è stato effettuato il positive test, che consiste nella generazione della fattura per un determinato documento, che è stato portato a termine con successo e senza anomalie; il negative test non è stato effettuato, poiché il programma non permette di provare a generare la fattura di un documento per cui è già stata creata, duenque sarebbe stato impossibile effettuare questo tipo di test.

3.3.5 Test delle IPE

Un IPE, come scritto nel secondo capitolo, è un qualsiasi tipo di documento prodotto dall'azienda cliente che viene utilizzato dai revisori per effettuare le loro valutazioni, di conseguenza è necessario testarlo per verificare che le informazioni all'interno siano corrette, altrimenti potrebbero esserci delle distorsioni nelle analisi sul bilancio. Come per gli ITAC anche per le IPE sono i colleghi della revisione che ci hanno chiesto di testare determinati report al fine di garantire la correttezza delle informazioni, almeno

per quanto riguarda l'elaborazione dell'IPE da parte dell'applicativo. Dei sei rischi relativi alle IPE elencati nel secondo capitolo noi, in quanto revisori dei sistemi informativi, testiamo soltanto quelli relativi alla generazione del report da parte del programma informatico, per verificare che funzioni correttamente.

Per valutare che l'applicativo operi senza effettuare errori il nostro obiettivo è quello di analizzare un determinato report ed in seguito ricercare lo stesso tipo di informazioni contenute in esso attraverso un percorso diverso, affinché sia possibile verificare che le informazioni siano le stesse e di conseguenza poter affermare che il programma estrae correttamente le informazioni.

Di seguito verrà mostrato il test di completezza ed accuratezza di un report riguardante delle vendite nel mese di giugno, che è stato estratto da un Data Warehouse che si appoggia sul sistema SAP, di conseguenza sull'applicativo SAP è stato possibile trovare i dati originali che sono stati estratti sul documento. Il test consiste nel verificare che i dati riportati nell'IPE sono gli stessi che si possono trovare su SAP per quelle determinare vendite in quel periodo.

Test IPE.

In **figura 26** i dettagli dell'IPE testato.

IPE
REPORT> [redacted]
Report Name (M): [redacted] Application name (M): SAP [redacted] Control Owner (M): [redacted] Technical report name (O): [redacted] Report Description (O)

Figura 26: informazioni sull'IPE in esame.

È stato estratto il report [redacted] relativo al periodo di giugno 2019 per la persona giuridica [redacted].

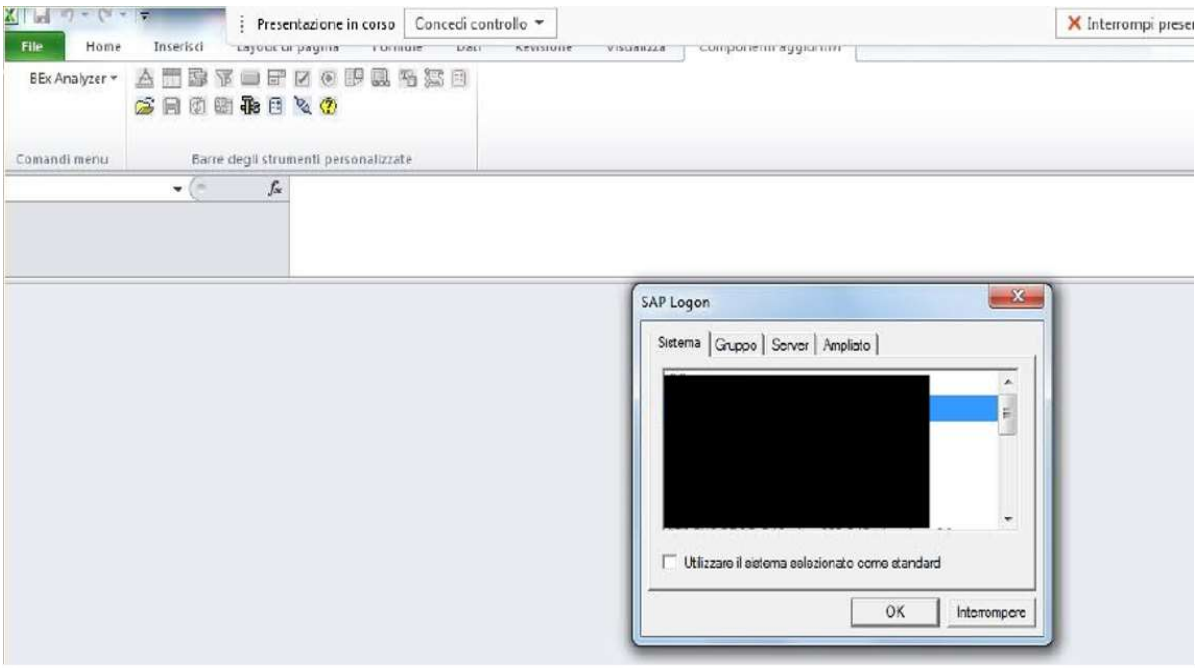


Figura 27: estrazione del report PT1

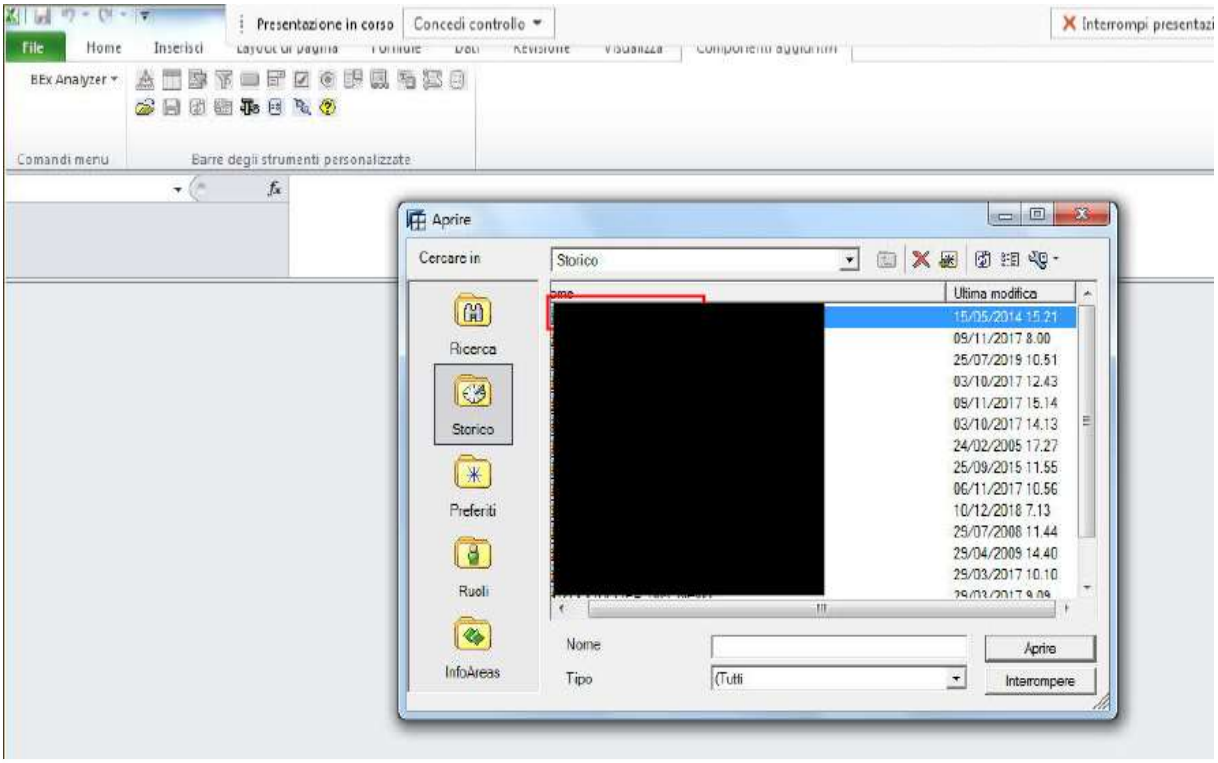


Figura 28: estrazione del report PT2

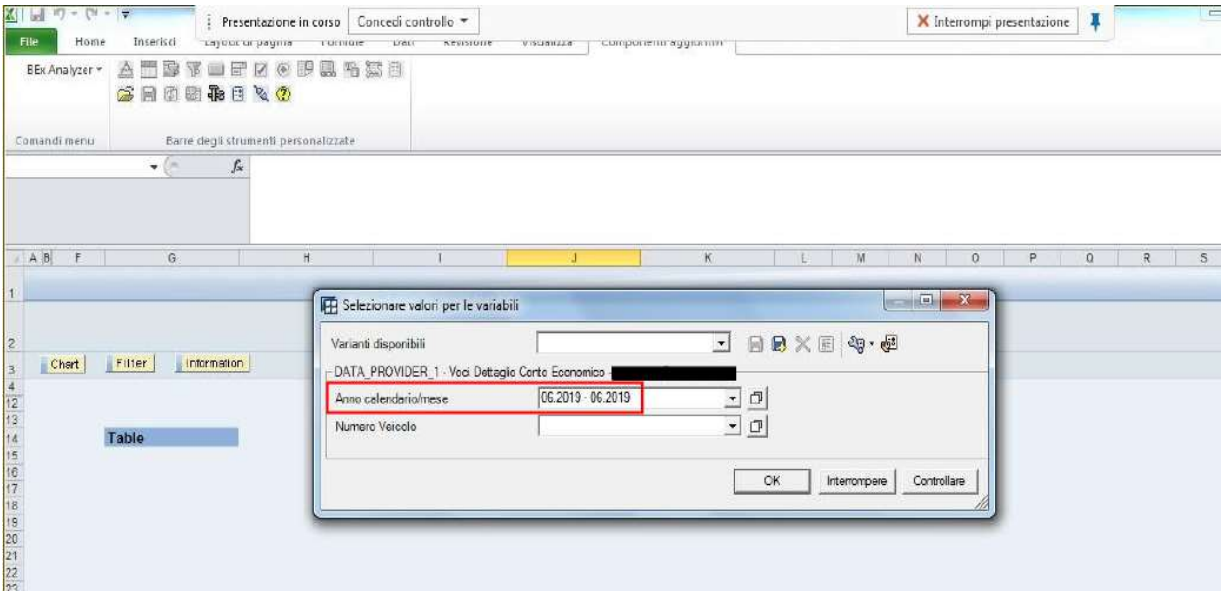


Figura 29: selezione del periodo di riferimento.

È stato selezionato il periodo di giugno. Il report contiene una serie di informazioni riguardo alle vendite, a noi interessano soltanto quelle di una determinata attività. Il numero di unità vendute è 7.110 e il fatturato relativo è 88.416.183 €

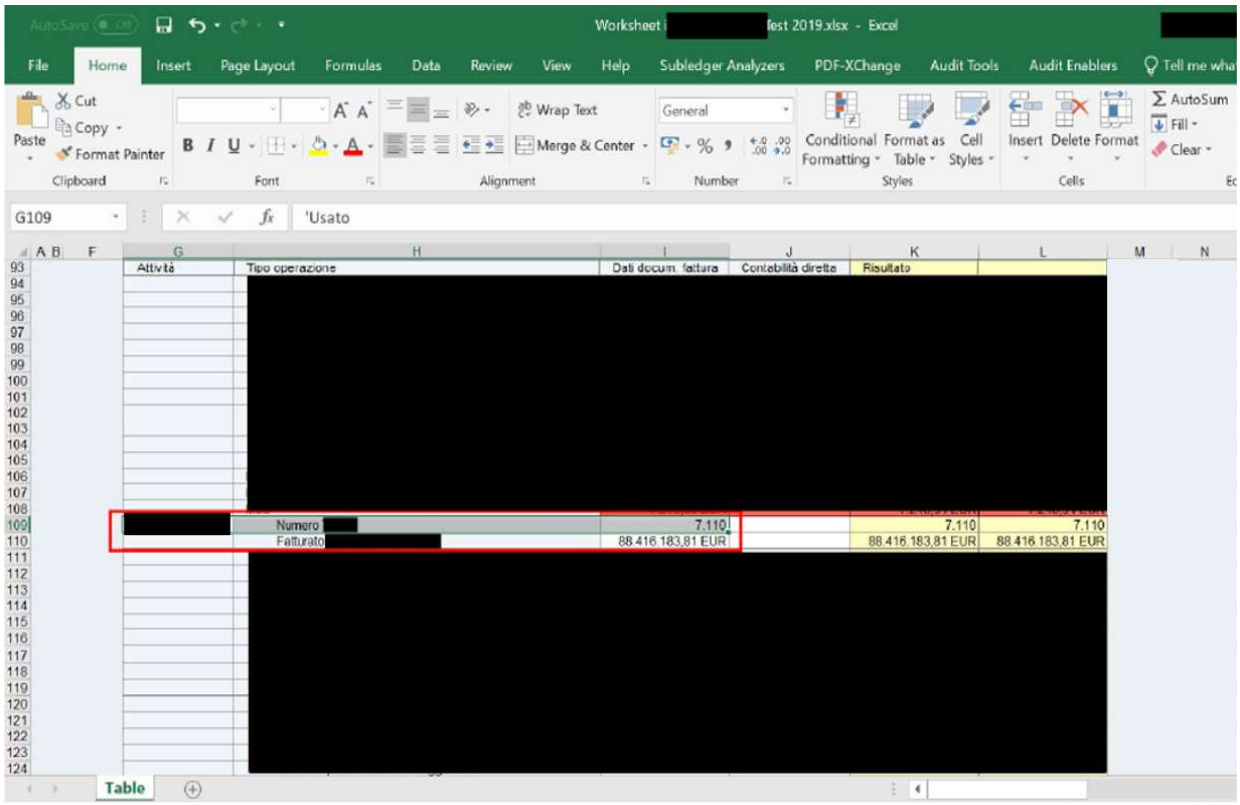


Figura 30: estrazione del report.

Per verificare la consistenza delle informazioni contenute nell' IPE sono stati estratti i dati con gli stessi parametri dal database di SAP X[redacted]:

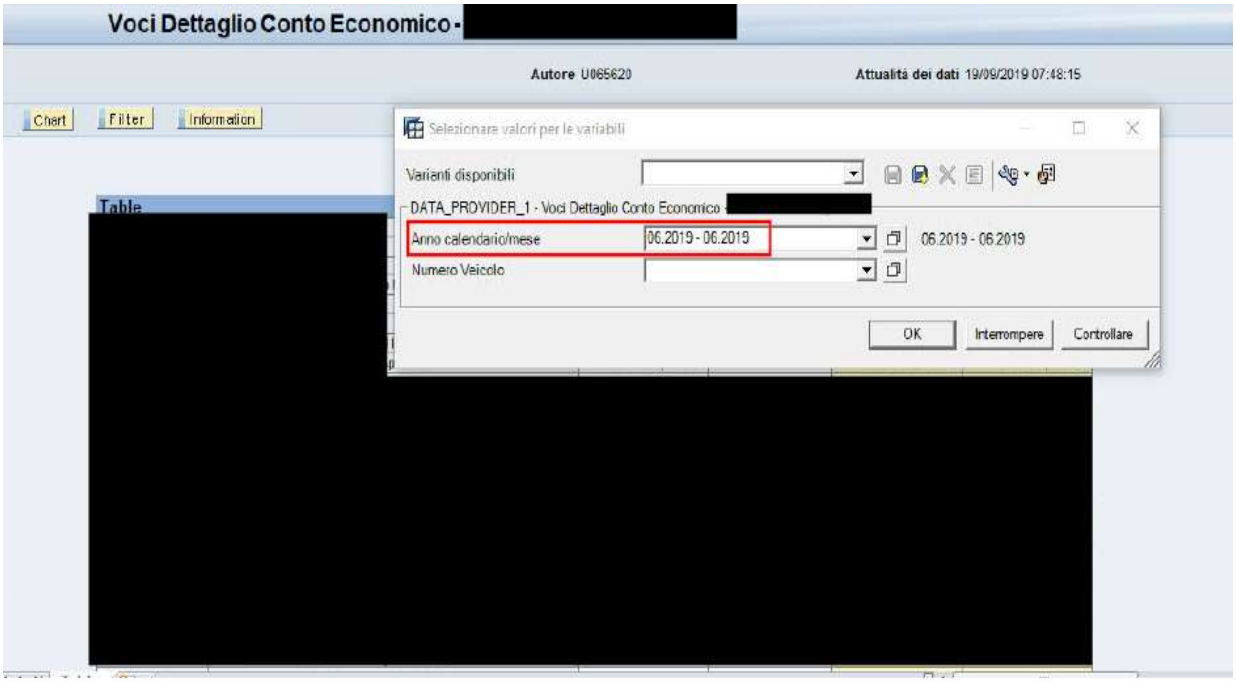


Figura 31: selezione del periodo di giugno.

SAP [redacted] non consente di selezionare più campi contemporaneamente, quindi sono stati estratti i due campi chiave "Numero" e "Fatturato":

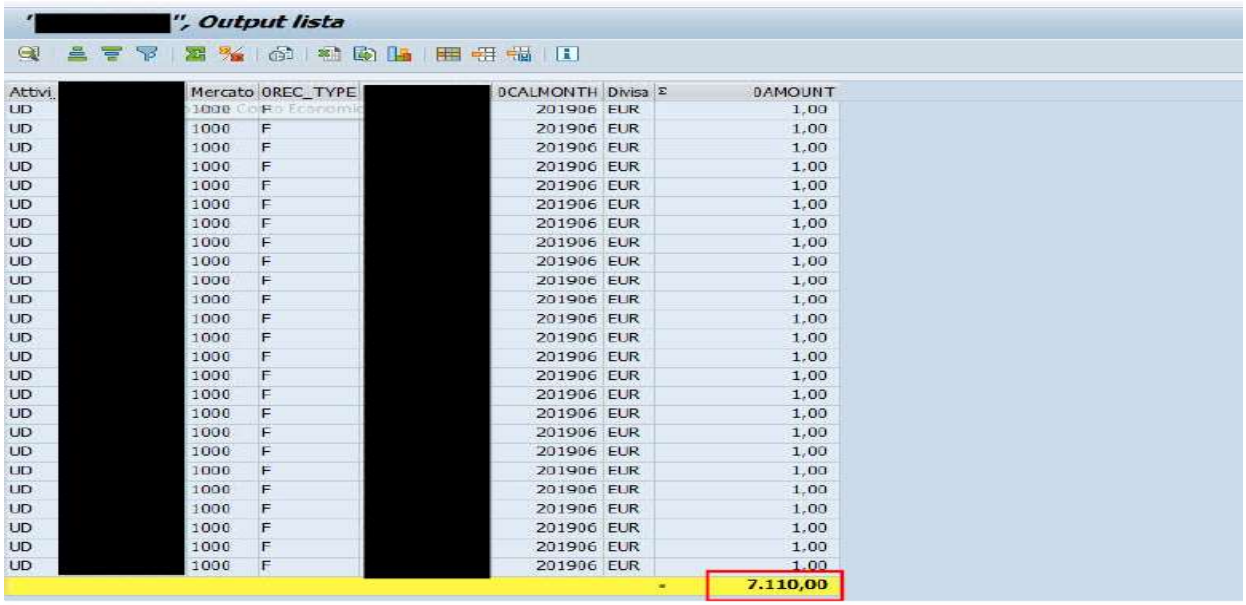


Figura 32: selezione del campo "Numero" su SAP.

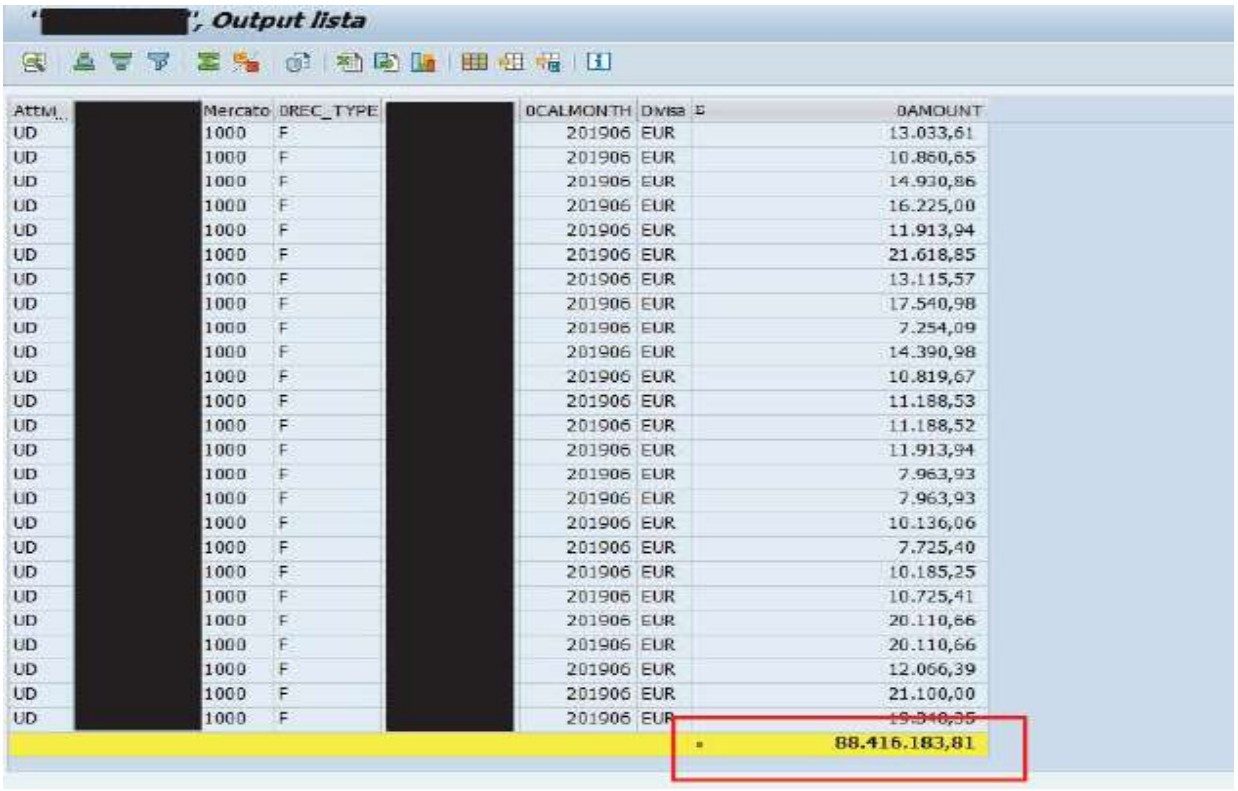


Figura 33: selezione del campo "Fatturato" su SAP

Confrontando i numeri del report e del database si può comprendere che sono gli stessi, di conseguenza si può concludere che il test della completezza dell'IPE sia positivo. In seguito, viene testata anche l'accuratezza dell'IPE, per fare ciò si confronta il valore specifico di una singola voce del report, con il corrispettivo valore che ha su SAP. È possibile verificare soltanto l'accuratezza puntuale confrontando soltanto una voce del report poiché il sistema è sotto una serie di controlli ITGC effective. È stato estratto casualmente l'articolo 0000215235 sia dal report che dal database. Di seguito le evodenze:

Report - Fatturato Lordo [redacted] --> 1.010,00€

Report - Fatt. Compl [redacted] --> 130,00€

Report - Totale Fatturato Lordo --> 1.140,00€

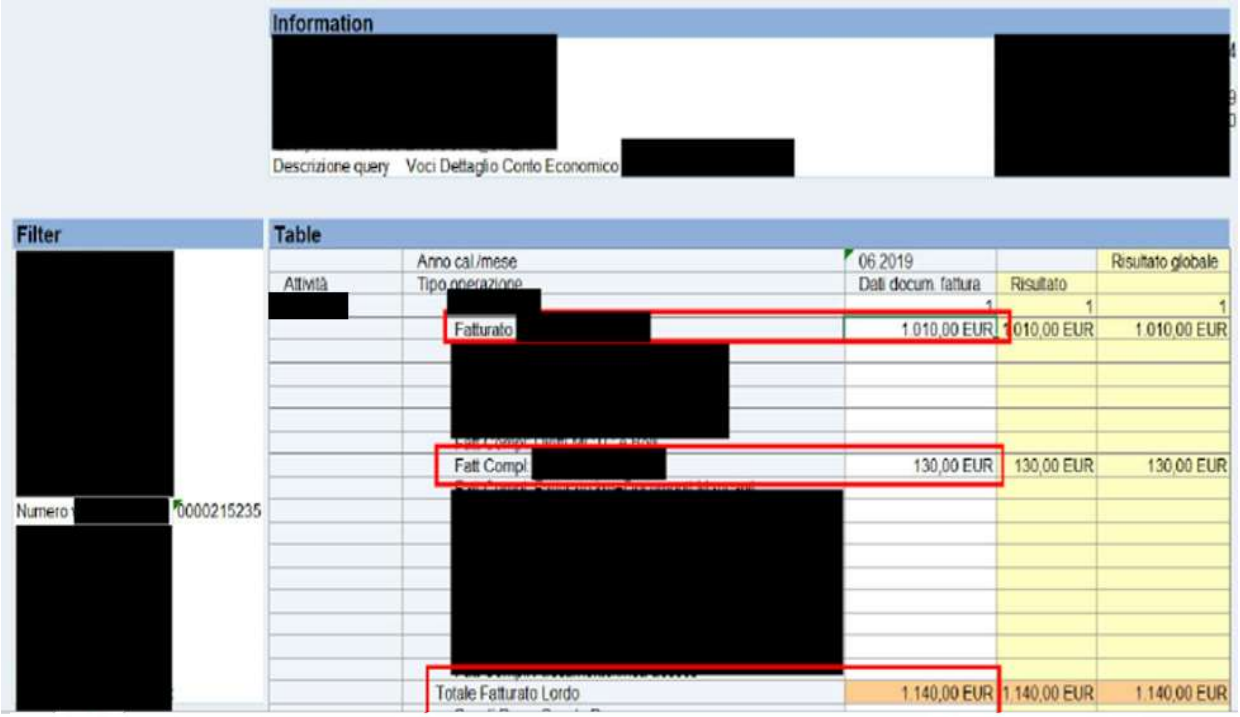


Figura 34: estrazione dell'item 0000215235 dal report

DB - Fatturato Lordo [redacted] --> 1.010,00€

DB - Fatt. Compl [redacted] --> 130,00€

DB - Totale Fatturato Lordo --> 1.140,00€

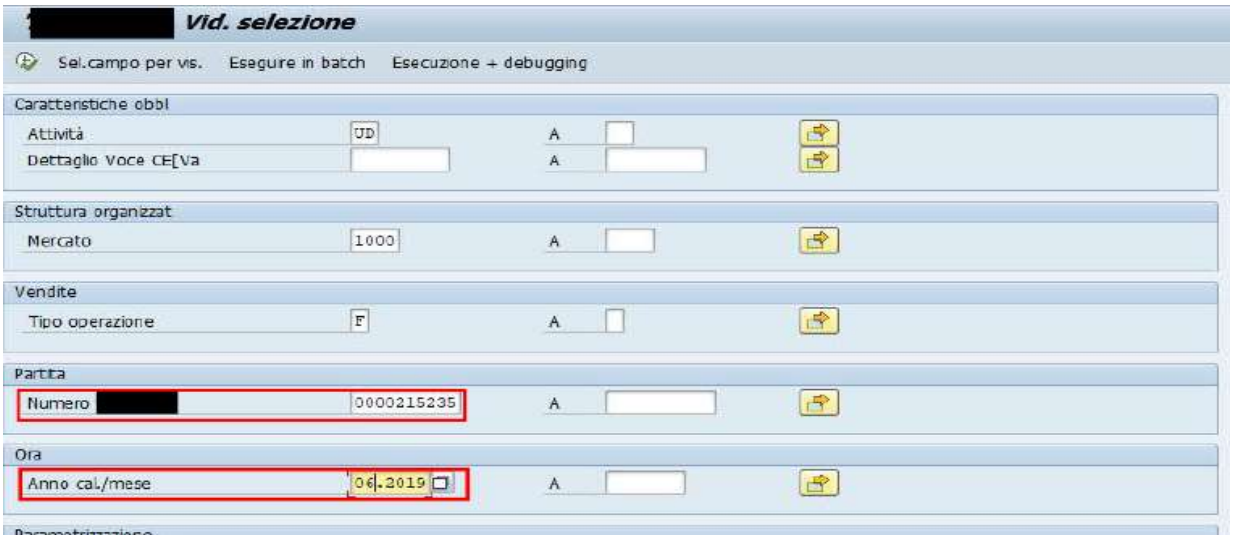


Figura 35: comandi di estrazione dell'item 0000215235 da SAP

Figura 36: estrazione dell'item 0000215235 da SAP

Il valore estratto dal report e quello estratto dal Database sono identici dunque anche il test sull'accuratezza è positivo, di conseguenza è possibile affermare che il sistema IT generi il report correttamente e dunque può essere utilizzato dal personale di revisione contabile per effettuare le loro analisi.

3.3.6 Conclusione del progetto di revisione dei sistemi informativi

Una volta terminata la fase di test di ITGC, ITAC e IPE il processo di audit IT è pressoché concluso. È da sottolineare che i tre test descritti in precedenza non sono svolti in maniera successiva, ma vengono eseguiti parallelamente, in base al materiale ricevuto dai referenti dell'azienda cliente.

Una volta formalizzati tutti i test viene effettuato un controllo sul lavoro svolto, in modo da verificare che non vi siano refusi nelle carte prodotte, prima di consegnarle ai colleghi di audit.

Durante il progetto di revisione non sono state trovate particolari anomalie nel funzionamento dell'ambiente IT dell'azienda cliente, infatti nessun processo è stato considerato ineffective, di conseguenza abbiamo comunicato ai colleghi revisori di bilancio che il sistema è stato considerato "Support", così che potessero confermare la loro strategia di audit di bilancio.
In seguito, i risultati ottenuti riguardo ai sistemi informativi sono stati riportati anche alla funzione IT della società cliente, presentando sia gli aspetti che andavano bene sia quelli che andavano meno bene, in modo che la società possa migliorarsi e possa avere le indicazione di come agire per continuare a migliorare la propria governance IT. Una volta comunicati i risultati alla società cliente e ai colleghi revisori il processo di IT audit può considerarsi concluso.
Il vero processo di revisione dell'azienda sarebbe terminato con la lettera di opinion firmata dal partner di EY, mandata in seguito alla conclusione da parte dei colleghi revisori delle loro analisi riguardanti il bilancio e i controlli interni, tuttavia non ho potuto assistere a questa fase del processo poiché il mio tirocinio si è concluso prima della data stabilita per la firma sull'opinion, tuttavia i nostri compiti siamo riusciti a portarli a termine entro le scadenze a noi imposte nonostante i vari ritardi e problemi causati dall'emergenza sanitaria.

3.4 Conclusioni

In conclusione, la mia esperienza nell'azienda EY Advisory S.p.A., nonostante tutti i problemi che sono sopraggiunti dovuti alla situazione che si sta attraversando in questo periodo e che ci ha costretti a lavorare da casa, è stata positiva. Innanzitutto perché la professione di IT audit non incontra particolari difficoltà nello svolgimento da remoto, perlomeno nel breve periodo, infatti lo "smart working" era già stato adottato dall'azienda prima dell'emergenza sanitaria; in secondo luogo perché ho svolto la formazione durante il mese trascorso in ufficio e per i dubbi e le domande che mi sono sopraggiunti durante il periodo di lavoro da casa i colleghi sono stati sempre disponibili e presenti per guidarmi nel lavoro attraverso i mezzi di telecomunicazione. Lavorare presso una società di consulenza porta con sé degli aspetti positivi, ma anche negativi. Innanzitutto, l'ambiente di lavoro è molto giovane, il che permette una facile integrazione per una persona che ha appena terminato l'università. Un altro aspetto da considerare sono le competenze acquisite durante l'esperienza di lavoro, infatti io ho ampliato il mio bagaglio di conoscenze, sia tecniche, poiché ho affinato le mie capacità con strumenti informatici che già conoscevo ed ho appreso ad utilizzarne di nuovi, che al giorno d'oggi sono fondamentali; sia culturali poiché, durante il lavoro e gli incontri effettuati, ho imparato molto a riguardo della struttura IT di un'azienda. Uno svantaggio del lavoro in una società di consulenza, in particolare una di revisione, è quello di essere assegnati a più clienti contemporaneamente, di conseguenza è richiesto un certo grado di elasticità mentale per poter seguire in maniera efficiente più clienti. Un altro svantaggio è quello dipendere dal cliente per svolgere il proprio lavoro, di conseguenza potrebbero esserci dei periodi scarichi di lavoro, alternati a periodi nei quali è necessario rimanere più a lungo del previsto sul lavoro per rispettare le scadenze. Infine, un ultimo aspetto negativo è quello della gestione dello stress, infatti quello del consulente è un lavoro che spesso riceve pressioni dall'esterno, ad esempio a ridosso delle scadenze di consegna di un progetto, il che richiede una buona capacità di gestione dello stress. In conclusione, personalmente, consiglierei ad un neolaureato di svolgere un'esperienza presso una società di consulenza.

Appendice 1

EY
Building a better working world

Reconta Ernst & Young S.p.A.
Via Po, 32
00198 Roma

Tel: +39 06 324751
Fax: +39 06 32475504
ey.com

Relazione della società di revisione sulla revisione limitata del Bilancio di Sostenibilità del Gruppo ACEA al 31 dicembre 2013

Agli azionisti della ACEA S.p.A.

1. Abbiamo effettuato la revisione limitata del Bilancio di Sostenibilità (di seguito il "Bilancio") della ACEA S.p.A. e sue controllate (di seguito "Gruppo ACEA") al 31 dicembre 2013. La responsabilità della redazione del Bilancio in conformità alle "Linee guida per il reporting di sostenibilità 3.1" definite nel 2011 dal GRI-*Global Reporting Initiative*, integrate dagli indicatori previsti dal supplemento *"Sustainability Reporting Guidelines & Electric Utilities Sector Supplement* (EUSS)" definito nel 2009 dal GRI, indicate nel paragrafo "Nota Metodologica", compete agli Amministratori della ACEA S.p.A., così come la definizione degli obiettivi del Gruppo ACEA in relazione alla performance di sostenibilità e alla rendicontazione dei risultati conseguiti. Compete altresì agli Amministratori della ACEA S.p.A. l'identificazione degli stakeholder e degli aspetti significativi da rendicontare, così come l'implementazione e il mantenimento di adeguati processi di gestione e di controllo interno relativi ai dati e alle informazioni presentati nel Bilancio. È nostra la responsabilità della redazione della presente relazione in base al lavoro svolto.
2. Il nostro lavoro è stato svolto secondo i criteri per la revisione limitata indicati nel principio "*International Standard on Assurance Engagements 3000 - Assurance Engagements other than Audits or Reviews of Historical Financial Information*" ("ISAE 3000"), emanato dall'*International Auditing and Assurance Standard Board*. Tale principio richiede il rispetto dei principi etici applicabili "*Code of Ethics for Professional Accountants*" dell'*International Federation of Accountants* ("IFAC"), compresi quelli in materia di indipendenza, nonché la pianificazione e lo svolgimento del nostro lavoro al fine di acquisire una limitata sicurezza, inferiore rispetto a un revisione completa, che il Bilancio non contenga errori significativi. Un incarico di revisione limitata del Bilancio consiste nell'effettuare colloqui, prevalentemente con il personale della società responsabile per la predisposizione delle informazioni presentate nel Bilancio, analisi del Bilancio ed altre procedure volte all'acquisizione di evidenze probative ritenute utili. Le procedure effettuate sono riepilogate di seguito:
    a. comparazione tra i dati e le informazioni di carattere economico-finanziario riportati nel Bilancio e i dati e le informazioni inclusi nel Bilancio Consolidato del Gruppo ACEA al 31 dicembre 2013, sul quale è stata emessa la relazione ai sensi degli artt. 14 e 16 del D.Lgs. 27.1.2010, n. 39 in data 30 aprile 2014;
    b. analisi delle modalità di funzionamento dei processi che sottendono alla generazione, rilevazione e gestione dei dati quantitativi inclusi nel Bilancio. In particolare, abbiamo svolto le seguenti procedure:
        - interviste e discussioni con il personale della ACEA S.p.A., della ACEA Illuminazione Pubblica S.p.A., della ACEA Ato2 S.p.A., della A.R.I.A S.r.l. e della ACEA Produzione S.p.A. al fine di raccogliere informazioni circa il sistema informativo, contabile e di reporting in essere per la predisposizione del Bilancio, nonché circa i processi e le procedure di controllo interno che supportano la raccolta, l'aggregazione, l'elaborazione e la trasmissione dei dati

Building a better working world

e delle informazioni alla funzione responsabile della predisposizione del Bilancio;

- analisi a campione della documentazione di supporto alla predisposizione del Bilancio, al fine di ottenere evidenza dei processi in atto, della loro adeguatezza e del funzionamento del sistema di controllo interno per il corretto trattamento dei dati e delle informazioni in relazione agli obiettivi descritti nel Bilancio;

c. analisi della conformità delle informazioni qualitative riportate nel Bilancio alle linee guida identificate nel paragrafo 1. della presente relazione e della loro coerenza interna, con particolare riferimento alla strategia, alle politiche di sostenibilità e all'identificazione degli aspetti significativi per ciascuna categoria di stakeholder;

d. analisi del processo di coinvolgimento degli stakeholder;

e. ottenimento della lettera di attestazione, sottoscritta dal legale rappresentante della ACEA S.p.A. sulla conformità del Bilancio alle linee guida indicate nel paragrafo 1., nonché sull'attendibilità e completezza delle informazioni e dei dati in esso contenuti.

La revisione limitata ha comportato un'estensione di lavoro inferiore a quella di una revisione completa svolta secondo l'ISAE 3000 e, conseguentemente, non ci consente di avere la sicurezza di essere venuti a conoscenza di tutti i fatti e le circostanze significativi che potrebbero essere identificati con lo svolgimento di una revisione completa.

Per quanto riguarda i dati e le informazioni relative al Bilancio di Sostenibilità dell'esercizio precedente presentati a fini comparativi, si fa riferimento alla relazione emessa da altra società in data 27 marzo 2013.

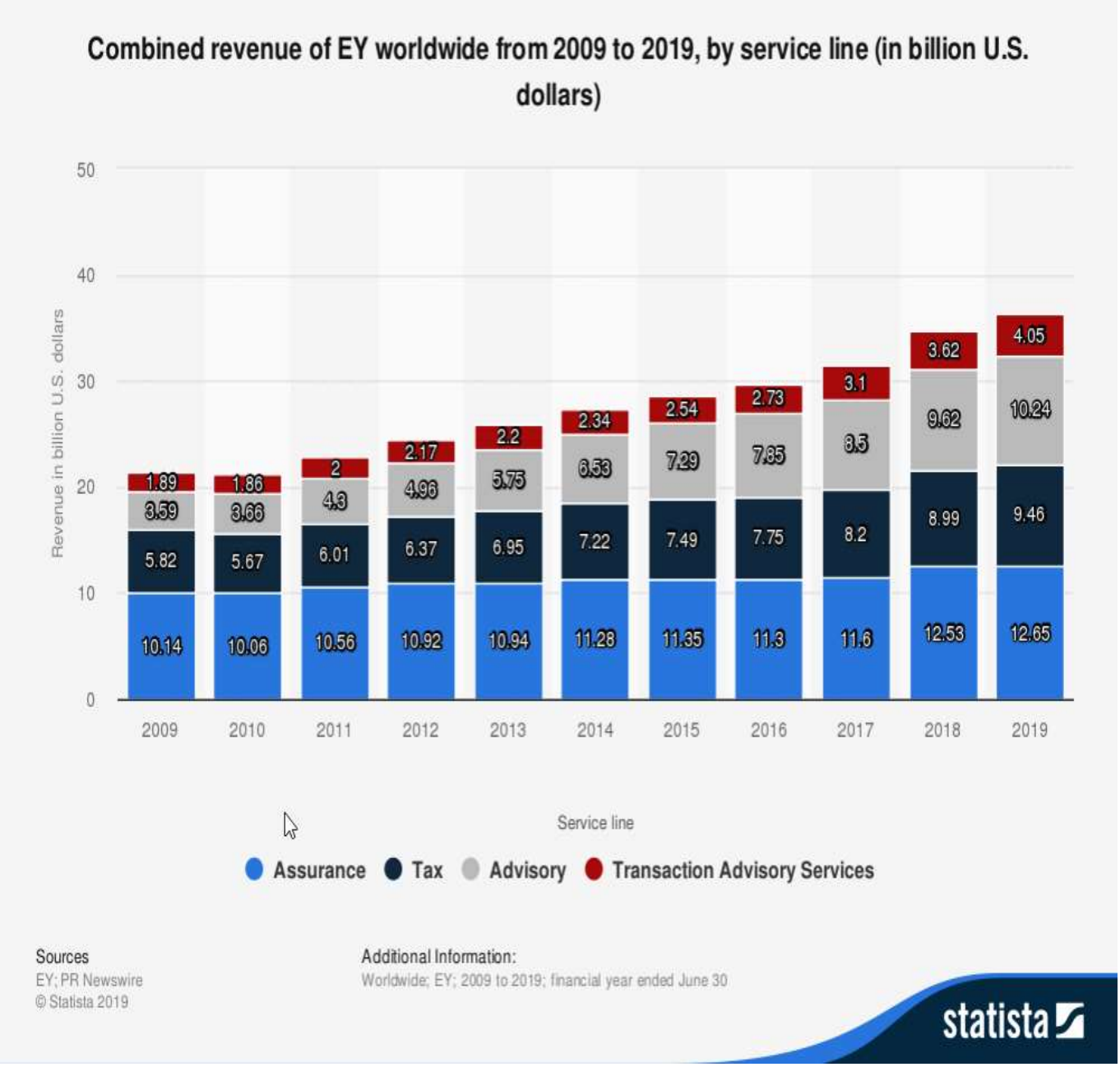
3. Sulla base di quanto svolto non sono pervenuti alla nostra attenzione elementi che ci facciano ritenere che il Bilancio di Sostenibilità del Gruppo ACEA al 31 dicembre 2013 non sia stato redatto, in tutti gli aspetti significativi, in conformità alle "Linee guida per il reporting di sostenibilità 3.1" definite nel 2011 dal GRI-*Global Reporting Initiative*, integrate dagli indicatori previsti dal supplemento *"Sustainability Reporting Guidelines & Electric Utilities Sector Supplement* (EUSS)" definito nel 2009 dal GRI, come descritto nel paragrafo "Nota Metodologica" del Bilancio.

Roma, 30 aprile 2014

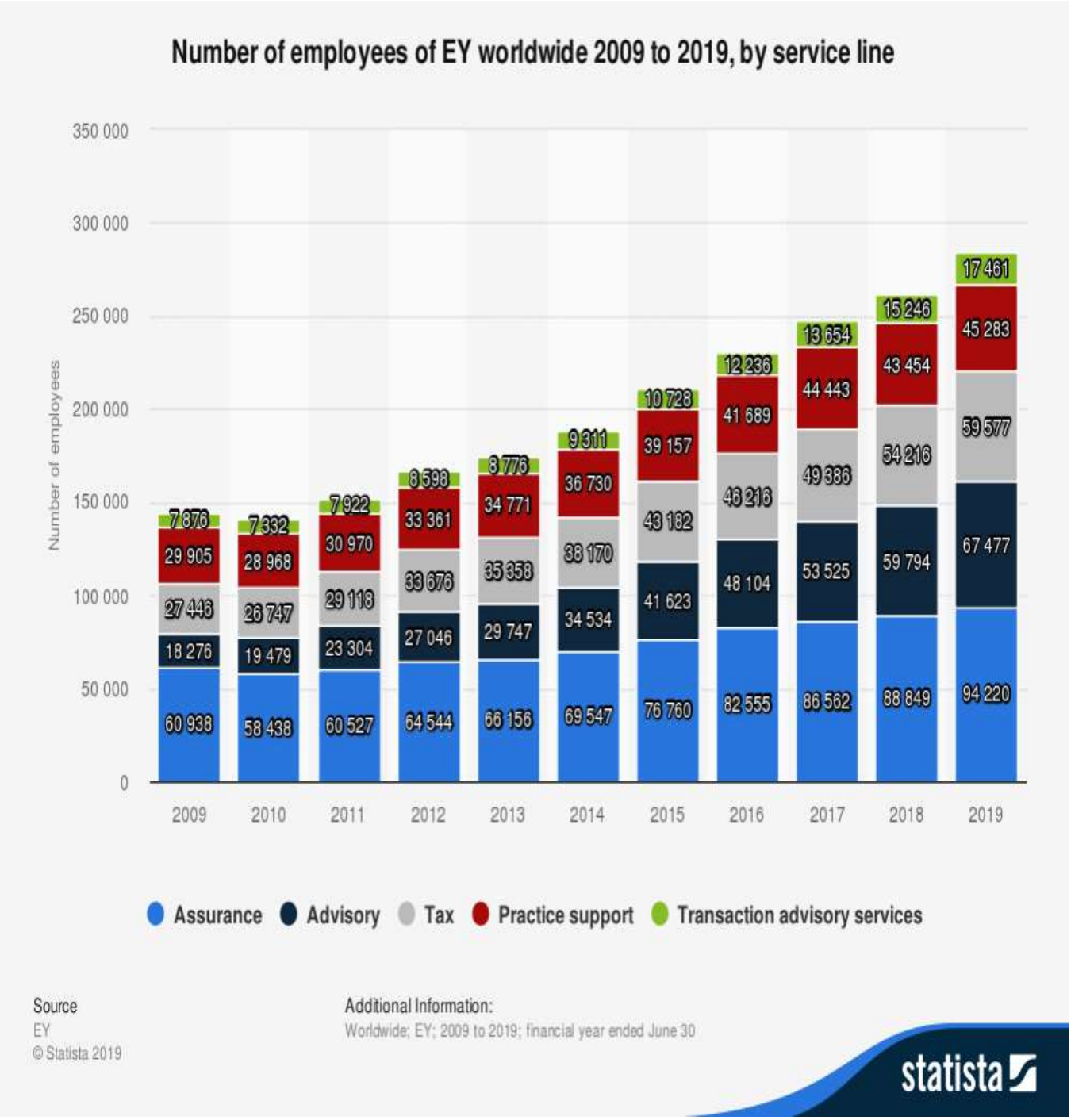
Reconta Ernst & Young S.p.A.

Filippo Maria Aleandri
(Socio)

Appendice 2


Combined revenue of EY worldwide from 2009 to 2019, by service line (in billion U.S. dollars)
Revenue in billion U.S. dollars
50
40
30
20
10
0
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
1.89
3.59
5.82
10.14
1.86
3.66
5.67
10.06
2
4.3
6.01
10.56
2.17
4.96
6.37
10.92
2.2
5.75
6.95
10.94
2.34
6.53
7.22
11.28
2.54
7.29
7.49
11.35
2.73
7.85
7.75
11.3
3.1
8.5
8.2
11.6
3.62
9.62
8.99
12.53
4.05
10.24
9.46
12.65
Service line
Assurance
Tax
Advisory
Transaction Advisory Services
Sources
EY; PR Newswire
© Statista 2019
Additional Information:
Worldwide; EY; 2009 to 2019; financial year ended June 30
statista

Appendice 3


Number of employees of EY worldwide 2009 to 2019, by service line
Number of employees
350 000
300 000
250 000
200 000
150 000
100 000
50 000
0
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
60 938
58 438
60 527
64 544
66 156
69 547
76 760
82 555
86 562
88 849
94 220
18 276
19 479
23 304
27 046
29 747
34 534
41 623
48 104
53 525
59 794
67 477
27 446
26 747
29 118
33 676
35 358
38 170
43 182
46 216
49 386
54 216
59 577
29 905
28 968
30 970
33 361
34 771
36 730
39 157
41 689
44 443
43 454
45 283
7 876
7 332
7 922
8 598
8 776
9 311
10 728
12 236
13 654
15 246
17 461
Assurance
Advisory
Tax
Practice support
Transaction advisory services
Source
EY
© Statista 2019
Additional Information:
Worldwide; EY; 2009 to 2019; financial year ended June 30
statista

Appendice 4: elenco degli Enti di Interesse Pubblico revisionati da EY S.p.A. nel Fiscal Year 2019

Elenco degli Enti di Interesse Pubblico oggetto di revisione legale

In allegato alla presente relazione, si riporta l'elenco degli Enti di Interesse Pubblico i cui bilanci sono stati oggetto di revisione legale da parte di EY S.p.A. nell'esercizio sociale chiuso al 30 giugno 2019.

A2A S.p.A.

Acotel Group S.p.A.

Aeroporti di Roma S.p.A.

Aeroporto Guglielmo Marconi di Bologna S.p.A.

Agresti 6 SPV S.r.l.

Alleanza Assicurazioni S.p.A.

Ambienthesis S.p.A.

Amissima Assicurazioni S.p.A.

Amissima Vita S.p.A.

Arca Assicurazioni S.p.A.

Arca Vita S.p.A.

Argo Mortgage 2 S.r.l.

Argoglobal Assicurazioni S.p.A.

Asset-Backed European Securitisation transaction Fifteen S.r.l.

Asset-Backed European Securitisation Fourteen S.r.l.

Asset-Backed European Securitisation Ten S.r.l.

Asset-Backed European Securitisation Twelve S.r.l.

Assicuratrice Val Piave S.p.A.

Assicurazioni Generali S.p.A.

Assimoco S.p.A.

Assimoco Vita S.p.A.

Banca Carige S.p.A. - Cassa di Risparmio di Genova e Imperia

Banca Cesare Ponti S.p.A.

Banca del Monte di Lucca S.p.A.

Banca della Nuova Terra S.p.A.

Banca di Cividale soc. Coop. per azioni

Banca di Credito cooperativo del basso Sebino soc. Coop.

Banca di Credito cooperativo di San Giovanni Rotondo soc. Coop.

Banca Euromobiliare S.p.A.

Banca Finnat Euramerica S.p.A.

Banca IFIS S.p.A.

Banca Leonardo S.p.A.

Banca Macerata S.p.A.

Banca Mediocredito del Friuli Venezia Giulia S.p.A.

Banca Monte dei Paschi di Siena S.p.A.

Banca per lo Sviluppo della Cooperazione di Credito S.p.A.

Banca Popolare di Sondrio Società cooperativa per azioni

Banca Reale S.p.A.

BasicNet S.p.A.

Bim Vita S.p.A.

Brunello Cucinelli S.p.A.

Buzzi Unicem S.p.A.

C.P.G. Società di cartolarizzazione a r.l.

CALEFFI S.p.A.

CARS ALLIANCE AUTO LOANS ITALY 2015 S.r.l.

Cassa di sovvenzioni e risparmio fra il personale della Banca d'Italia soc. Coop. per azioni

Cassa Lombarda S.p.A.

Cembre S.p.A.

Civitas SPV S.r.l.

COIMA RES S.p.A. Società di Investimento Immobiliare Quotata

Compagnia Italiana di Previdenza, Assicurazioni e Riassicurazioni S.p.A.

Compass Banca S.p.A.

Credemassicurazioni S.p.A.

CredemVita S.p.A.

Credico Finance 10 S.r.l.

Credico Finance 12 S.r.l.

Credico Finance 16 S.r.l.

Credico Finance 7 S.r.l.

Credico Finance 8 S.r.l.

Credico Finance 9 S.r.l.

Crédit Agricole Friuladria S.p.A.

Crédit Agricole Italia S.p.A.

Credito Emiliano S.p.A.

D.A.S. Difesa Automobilistica Sinistri - S.p.A. di Assicurazione

Danieli & C. Officine Meccaniche S.p.A.

Datalogic S.p.A.

De' Longhi S.p.A.

Dobank S.p.A.

Dominato Leonense S.r.l.

E.S.TR.A. S.p.A.

Emilia SPV S.r.l.

ENAV S.p.A.

ENEL S.p.A.

ENERVIT S.p.A.

Eni S.p.A.

ePRICE S.p.A.

Esprinet S.p.A.

Europ Assistance Italia S.p.A.

Falck Renewables S.p.A.

FCA Bank S.p.A.

FIDIA S.p.A.

Fiera Milano S.p.A.

Freni Brembo S.p.A.

Garofalo Health Care S.p.A.

Generali Italia S.p.A.

Genertel S.p.A.

Genertellife S.p.A.

Giglio Group S.p.A.

GIMA TT S.p.A.

Gruppo Mutuionline S.p.A.

HVL Bolzano S.r.l.

I.M.A. Industria Macchine Automatiche S.p.A.

ICCREA Banca S.p.A.

ICCREA Bancaimpresa S.p.A.

ICCREA SME Cart 2016 S.r.l.

Il Sole 24 ORE S.p.A.

Indigo Lease S.r.l.

Intercos S.p.A.

Interpump Group S.p.A.

Island Refinancing S.r.l.

ITAS Istituto Trentino Alto Adige per Assicurazioni Soc. Mutua di Assicurazioni

Juventus Football Club S.p.A.

KEDRION S.p.A.

Lanterna Finance S.r.l.

Molecular Medicine S.p.A.

MondoMutui Cariparma S.r.l.

MPS Leasing & Factoring, Banca per i Servizi Finanziari alle Imprese S.p.A.

MPS Capital Services Banca per le Imprese S.p.A.

Panariagroup Industrie Ceramiche S.p.A.

PLC S.p.A.

Pronto Assistance S.p.A.

Prysmian S.p.A.

Quarzo S.r.l.

Ratti S.p.A.

RBM Assicurazione Salute S.p.A.

Reply S.p.A.

Sabaf S.p.A.

Sagrantino Italy S.r.l.

Saipem S.p.A.

Salvatore Ferragamo S.p.A.

Saras S.p.A.

Schweizerische Hagel-Versicherungs-Gesellschaft Gmbh

Siena lease 20162 S.r.l.

SIENA MORTGAGES 07-5 S.p.A.

SIENA MORTGAGES 096 S.r.l.

SIENA MORTGAGES 10-7 S.r.l.

SIENA PMI 2015 S.r.l.

SIENA PMI 2016 S.r.l.

Società Reale Mutua di Assicurazioni S.p.A.

Stefanel S.p.A.

SUNRISE SPV 20 S.r.l.

SUNRISE SPV 40 S.r.l.

SUNRISE SPV 50 S.r.l.

SUNRISE S.r.l.

Ternienergia S.p.A.

Tesmec S.p.A.

Triboo S.p.A.

TXT e-solutions S.p.A.

V.E.R.I.T.A.S. S.p.A.

Wise Dialog Bank S.p.A.

Bibliografia e sitografia

About the PCAOB. (s.d.). Tratto da pcaobus.org: https://pcaobus.org//About/Pages/default.aspx

AIEA. (2006). *Il ruolo dell'IT nel progetto e nell'implementazione dei controlli interni per la predisposizione del reporting finanziario.* Milano: ISACA.

AIIA. (s.d.). *Definizione di IA*. Tratto da https://www.aiiaweb.it/definizione-di-internal-auditing#:~:text=Definizione%20di%20Internal%20Auditing,dell'efficienza%20dell'organizzazione.

Art. 154-bis Dirigente preposto alla redazione dei documenti contabili societari. (2005). Tratto da RicercaGiuridica: https://www.ricercagiuridica.com/codici/vis.php?num=24786&search=

Cassandrelli, S. (2006). *PICCOLE E MEDIE IMPRESE: PERCHE LA REVISIONE.* Tratto da sergio2017.

committee, S. a. (2006). *Final report of the advisory commitee on smaller public companies to the U.S. securities and exchange commission.* Washington DC.

Deloitte. (2018, Novembre). *General IT Controls - Risk and Impact.* Tratto da deloitte.com: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-general-it-controls-noexp.pdf

EconomiaAziendale. (s.d.). *PRINCIPI DI REDAZIONE DEL BILANCIO D'ESERCIZIO*. Tratto da EconomiaAziendale.net: https://www.economiaziendale.net/bilancio/principi_redazione_bilancio_esercizio.htm

EY. (2019). *Discover our service lines*. Tratto da https://www.fscareers.ey.com/service-lines/

EY. (2019). *Relazione di Trasparenza 2019.*

EY. (2020). *EY reports record global revenues of US$36.4b in 2019*. Tratto da https://www.ey.com/en_cy/news/2020-press-releases/01/ey-reports-record-global-revenues-in-2019#:~:text=EY%20today%20announces%20record%20combined%20global%20revenues%20of%20US%2436.4,financial%20year%20ended%20June%202019.

EY. (s.d.). *EY Canvas*. Tratto da Sito web di EY: https://www.ey.com/en_gl/audit/technology/canvas

Fortunato, S. (2004). Il provvedimento del Public Company Accounting Oversight Board. *Rivista dei Dottori Commercialisti*.

Gantz, S. (2014). In S. Gantz, *The basics of IT audit: purposes, processes, and pratical information.*

ISACA. (2009). *The Risk IT Framework.* USA.

ISACA. (2016). Tratto da isaca.org: https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpisatt

Kenton, W. (2019). *Internal Controls*. Tratto da Investopedia: https://www.investopedia.com/terms/i/internalcontrols.asp

Lander, G. P. (2004). What the Act Does - Applicability. In G. P. Lander, *What is Sarbanes-Oxley?* USA: McGraw - Hill.

LaRevisioneLegale. (2012). *Rilevazione ed analisi del sistema informatico*. Tratto da https://www.larevisionelegale.it/: https://www.larevisionelegale.it/wp-content/uploads/2012/02/c4.pdf

Moeller, R. (2010). In R. Moeller, *IT Audit, Control, and Security.* USA: Wiley.

Pampolini, K. (2017). *L'evoluzione della gestione informativa aziendale: benefici, criticità e supporto alle organizzazioni.* Venezia.

PCAOB. (2007). *Auditing Standard No. 5*. Tratto da pcaobus.org: https://pcaobus.org/Standards/Archived/PreReorgStandards/Pages/Auditing_Standard_5.aspx

Prampolini, N. (2011). *La legge 262/05 e le sue implicazioni*. Tratto da Aiea: https://www.aiea.it/sites/default/files/attivita/sds/verona_24_marzo_2011_prampolini_626.pdf

Presti, C. (2016). *L'INTEGRAZIONE DEL SISTEMA INFORMATIVO - CONTABILE: EVOLUZIONE STORICA E PROSPETTIVE FUTURE.* Pisa.

Protiviti. (2007). *GUIDE TO THE SARBANES-OXLEY ACT: Internal Control Reporting Requirements (Fourth Edition),* . Tratto da protiviti.com: https://www.protiviti.com/sites/default/files/united_states/insights/protiviti_section_404_faq_guide.pdf

SEC. (2006). *Final report of the advisory commitee on smaller public companies to the U.S. securities and exchange commission.* Washington DC.

SOX Section 906: Corporate Responsibility for Financial Reports. (2005). Tratto da sarbanes-oxley-101: https://www.sarbanes-oxley-101.com/SOX-906.htm

U. Gelinas, R. D. (2008). *Accounting Information Systems 8th edition.* Canada: Cengage Learning.

Un punto di riferimento nel sistema di controllo integrato. (s.d.). Tratto da Associazione Italiana Internal Auditors: https://www.aiiaweb.it/aiia-la-professione

Valsania, M. (2013, Dicembre 2). La madre di tutte le truffe contabili: lo scandalo Enron 12 anni dopo. *Il sole 24 ore*, p. 1.

Wikipedia. (s.d.). *Audit interno*. Tratto da Wikipedia: https://it.wikipedia.org/wiki/Audit_interno#:~:text=L'IS%20auditing%20(in%20italiano,norme%2C%20regolamenti%20o%20politiche%20interne.

Wikipedia. (s.d.). *Revisione contabile*. Tratto da Wikipedia: https://it.wikipedia.org/wiki/Revisione_contabile