POLITECNICO DI TORINO

Dipartimento di Ingegneria Gestionale e della Produzione

Corso di Laurea Magistrale in Ingegneria Gestionale

Tesi di Laurea Magistrale

L'evoluzione dell'Audit IT: dalle origini delle attività alle prospettive future in un progetto di revisione contabile

Relatore:

Prof. Luigi Buzzacchi

Candidato:

Davide D'Alò

Anno Accademico 2020-2021

Sommario

Abstract

Lo scopo di tale elaborato è quello di illustrare la figura dell'auditor IT, partendo da quello che è stato, nel quadro del sistema capitalistico, il percorso seguito fino ad oggi in tema di controlli nelle società quotate, per capire quali possano essere gli sviluppi in futuro, in un'ottica di costante miglioramento del sistema.

Si cercherà quindi di evidenziare quale sia stata l'evoluzione nel tempo dei controlli aziendali, partendo dal "sistema di controllo interno" con il quale si definisce, a livello di dottrina, quell'insieme delle "attività di verifica e riscontro che competono ad appositi organi e funzioni aziendali appartenenti all'organizzazione dell'impresa"[1].

Gli scandali finanziari degli ultimi decenni, accompagnati dal difficile periodo economico, hanno evidenziato la necessità di sviluppare degli organi di controllo con l'intento di sorvegliare l'attività ed avere una migliore trasparenza e gestione delle società.

L'analisi in un primo momento partirà dalla trattazione del contesto internazionale. Il sistema di controllo vede la sua nascita negli Stati Uniti dove, tra gli anni '50 e '80, a seguito di un numero rivelante di fallimenti societari, nacque il bisogno di maggiori controlli: di conseguenza, tramite una dettagliata individuazione dei rischi e l'adozione di corrette norme di comportamento, furono adottate misure volte a mitigare il rischio di frodi.

In seguito, è stato redatto il "CoSO Report 1992" il primo documento con cui è stato elaborato un modello di riferimento per le realtà societarie, seguito nel nuovo secolo, da una serie di atti non meno importanti a partire dal Sarbanes - Oxley Act (SOA) e le ulteriori integrazioni del CoSO Report, con i quali il concetto di controllo interno è stato "inserito in quello più ampio di gestione dei rischi".[2]

Al termine di tale ricostruzione dell'evoluzione normativa in ambito di controlli, l'attenzione sarà posta sui sistemi informativi che, data la crescente complessità

[1] Gasparri, G. "*I controlli interni nelle società quotate. Gli assetti della disciplina italiana e i problemi aperti*", settembre 2013, Consob, Milano.
[2] Gasparri, G., *Op. cit*., settembre 2013.

dei processi aziendali, sono indispensabili per supportare la rendicontazione finanziaria e contabile e per garantire maggiore correttezza dei dati.

Con il tempo, infatti, il sistema informativo si è trasformato da semplice raccoglitore ed elaboratore di dati di natura contabile ed economica a polmone informativo principale di tutta l'azienda. Da qui l'importanza di monitorare i rischi che intaccano i sistemi informativi; ne consegue la necessità di una figura ad hoc, quale l'auditor IT, che fornisca valutazioni di adeguatezza e sicurezza dei sistemi informativi a supporto dei processi fiscali e contabili ed indichi mirati piani di miglioramento per aumentare l'efficacia e la robustezza dei sistemi IT. Sono descritte le procedure attuate per revisionare i controlli interni effettuati dalle società, al fine di garantire l'integrità delle informazioni finanziarie e contabili, promuovere la responsabilità e prevenire le frodi.

In conclusione, a fronte di un quadro completo del passato e del presente, nell'ultima parte Il focus dell'analisi verterà sul cambiamento tecnologico, sul suo impatto sulle strutture organizzative e su come ha inciso in termini di sicurezza societaria, rendendo necessaria l'adozione di un piano di audit per la Cyber Security.

Capitolo 1

1.1 Origini dell'internal auditor: dalla nascita alla comparsa del revisore esterno

L'attività del controllo interno vede le sue origini negli Stati Uniti alla fine degli anni 40; precedentemente all'interno della revisione contabile quest'attività non era stata necessaria, ma l'ingrandirsi delle dimensioni dei contesti aziendali aveva fatto sì che si sviluppasse una nuova modalità di controllo sui rendiconti finanziari al posto dell'utilizzo di verifiche campionarie.

Data l'importanza del ruolo che dovevano assumere i controlli interni era necessario che questi fossero adeguati ed efficaci in modo da trasmettere quelle che vengono definite come "garanzie per assicurare la veridicità e la completezza dei documenti contabili"[3].

Successivamente, alla fine degli anni '50 si sviluppa una nuova concezione di auditing meno circoscritta alla sola rendicontazione finanziaria: nel 1958 viene redatto dal "Committee on Auditing Procedure dell'American Institute of Certified Public Accountants" (AICPA) lo "Statement on Auditing Procedure No. 29", nonché una dichiarazione con lo scopo di chiarire il compito relativo all' auditor interno rispetto al complesso della revisione contabile ovvero definire quel contesto di attività che riguardano sia "l'efficienza operativa e l'aderenza alle politiche gestionali"[4] sia quelle che mirano alla rendicontazione finanziaria.

Ancora dopo, nel 1972 viene ripresa la definizione di auditing con la pubblicazione della nuova "Statement on Auditing Procedure No. 54": si formula una nuova dichiarazione del controllo interno visto come un "piano di organizzazione, procedure e documentazione"[5] volto alla gestione delle modalità con cui l'amministrazione esprime il proprio consenso sul modus operandi, mentre la revisione contabile viene vista come un controllo riguardante solo la tutela dei beni aziendali e garante della credibilità della documentazione finanziaria.

[3] Gasparri, G., *Op. cit*., settembre 2013.
[4] Gasparri, G., *Op. cit*., settembre 2013.
[5] Gasparri, G., *Op. cit*., settembre 2013.

Proprio quest'ultima definizione viene ripresa verso la fine degli anni '70 con il "Foreign Corrupt Practices Act", per cui il controllo interno diviene "un requisito per le società quotate ai sensi del Securities Exchange Act del 1934"[6].

Nonostante ciò nel decennio seguente si vede il succedersi di una serie di fallimenti societari, dovuti a gestioni fraudolenti, da fare sì che nel 1985, "con il patrocinio congiunto di cinque importanti associazioni professionali statunitensi"[7], viene a costituirsi la "Treadway Commission" (il cui nome completo è "National Commission on Fraudolent Financial Reporting"), commissione con l'incarico di analizzare i possibili fattori che possono portare al falso in bilancio.
Appena due anni dopo nel 1987 viene pubblicato il "Treadway Report" ("Report on Fraudulent Financial Reporting"), che mette in rilievo come il controllo interno con la sua attività possa agire come barriera per prevenire il verificarsi di frodi finanziarie. In questo report si cerca di dimostrare come le frodi non venivano effettivamente analizzate in maniera adeguata, ovvero come tentativo di ottenere guadagni illeciti, ma come una concezione errata che vi era nell'attività del controllo interno visto come "insieme di autonome attività ispettive"[8].

Nasce la necessità di definire uno standard con lo scopo di poter indicare un processo costituito prima da una cosiddetta "mappatura dei rischi", per cui vengono individuati gli ambiti più soggetti a rischio, seguita poi dall'adozione di "protocolli comportamentali che guidino l'intera organizzazione e permettano di agire sulle aree ritenute più esposte al rischio"[9].
Si viene a formare quindi "un apposito sottogruppo, denominato "Committee of Sponsoring Organizations of the Treadway Commission" (CoSO), con il compito di realizzare un guida di riferimento ovvero di definire una procedura standard per i controlli interni.
Successivamente nel 1992, la definizione di tale framework è stata commissionata alla società di revisione Coopers & Lybrand (nonché l'attuale

[6] Gasparri, G., *Op. cit*., settembre 2013.
[7] Gasparri, G., *Op. cit*., settembre 2013.

[8] Gasparri, G., *Op. cit*., settembre 2013.
[9] Gasparri, G., *Op. cit*., settembre 2013.

società PricewaterhouseCoopers) che, tramite un reciproco rapporto d'interesse con figure come "amministratori e dirigenti di imprese di diverse dimensioni, pubbliche e private, docenti universitari, autorità di vigilanza, revisori esterni ed interni", ha elaborato il cosiddetto "CoSO Report - Internal Control: Integrated Framework".[10]

1.2 Il CoSO Report del 1992

"Il CoSO framework è stato progettato per aiutare le aziende a stabilire, valutare e migliorare il loro controllo interno"[11]; le varie frodi societari hanno suscitato la necessità di dover razionalizzare il Sistema di Controllo Interno e il Sistema di Gestione dei Rischi, che è divenuto un elemento sempre più imprescindibile in ottica del contenimento dei costi, partendo dall'analisi e dalla riprogettazione di ruoli, compiti e responsabilità, attività da svolgere, sistemi informativi da utilizzare ed implementare, in ottica sempre più integrata.

La descrizione data di tale framework ha lo scopo di permettere alle varie organizzazioni di avere un modello a cui fare riferimento nel momento in cui decidessero di implementare tale sistema: il controllo interno risulta quindi essere "un processo, svolto dal consiglio di amministrazione, dai dirigenti e da altri operatori della struttura aziendale, che si prefigge lo scopo di fornire una ragionevole sicurezza sulla realizzazione dei seguenti obiettivi:

- efficacia ed efficienza delle attività operative;
- attendibilità delle informazioni di bilancio;
- conformità alle leggi e ai regolamenti in vigore"[12] .

Da tale definizione si possono dedurre alcuni importanti concetti[13]: innanzitutto, il controllo interno è un processo che avviene nel continuo, per cui non si realizza attraverso attività sporadiche; i provvedimenti posti in essere si caratterizzano

[10] Gasparri, G., *Op. cit*., settembre 2013.
[11] Olugbenro Y., *"COSO - An Approach to Internal Control Framework",* Agosto 2016.
[12] Gasparri, G., *Op. cit*., settembre 2013.
[13] Capparelli O., Lanzino L., *"Modelli di gestione del rischio e compliance ex D. Lgs. 231/2001"*, 2016, Wolters Kluwer, Milano.

infatti per la loro sistematicità e per il fatto di essere disegnati appositamente per la realtà aziendale a cui vengono applicati.

Alle società quotate, vengono quindi dettati dei suggerimenti per l'apparato aziendale che si occupa della redazione e alla verifica dei documenti informativi relativi all'ambito economico, con lo scopo di evidenziare la necessità di avere:

- un ambiente di controllo;
- un codice di comportamento;
- competenza efficiente dei comitati di auditing;
- una funzione di revisione interna attiva e obiettiva;
- l'intervento del management per verificare periodicamente l'efficacia del controllo interno;
- la predisposizione di un modello comune di controllo interno.[14]

Figura 1 Le componenti del Sistema di controllo interno (CoSo I)

Il framework è divenuto ben presto un riferimento soprattutto per coloro i quali si occupavano dell'informativa in ambito finanziario nelle aziende ed ha ottenuto un grande riconoscimento a livello mondiale, influenzando la redazione di diversi documenti relativi al sistema di controllo di vari Stati, come ad esempio l'Italia, in cui è considerato come una best practice.

Come visibile nella ***Figura 1***, il primo componente che definisce il "quadro" del CoSO è l'ambiente di controllo che è considerato la base di tutte le componenti del sistema di controllo interno"[15], in quanto determina la sensibilità dei membri

[14] Provasi, R., Guizzetti, C. (2019). L'evoluzione dei sistemi di controllo aziendale: dal controllo di gestione al controllo sulla governance. Economia Aziendale Online, Special Issue, 10(2), 257-271.

[15] Bava, F. "*La responsabilità amministrativa della società ed il sistema di controllo interno" in "Impresa Commerciale Industriale*" n. 1 del 2003.

dell'organizzazione nell'adottare specifiche procedure. L'ambiente di controllo è determinato da diverse variabili che sono descritte di seguito nella ***Tabella 1***:

Tabella 1 - Determinanti dell'ambiente di controllo

Variabili di tipo individuale	Caratteristiche delle risorse umane dell'azienda
Variabili di tipo sociale	Relazioni tra i vari soggetti aziendali
Variabili di tipo tecnico	Processi di trasformazione e tipo di tecnologia utilizzata
Variabili di tipo istituzionale	Governance aziendale

L'ambiente di controllo è l'insieme di standard, processi e strutture che forniscono la base per eseguire il controllo interno in tutta l'organizzazione: esercita una forte influenza sul modo in cui vengono strutturate le attività, stabiliti gli obiettivi e valutati i rischi. È il contesto nel quale il sistema è progettato e attuato; è un elemento chiave per assicurare una migliore governance; è costituito da azioni, politiche e procedure, che rispecchiano l'attitudine di tutti i componenti (alta direzione, CdA, ecc.) rispetto all'importanza del sistema di controllo interno. Un ambiente di controllo sarà ritenuto valido se, in esso, i soggetti sono consapevoli dell'importanza dei controlli.[16]

Per quanto riguarda la valutazione dei rischi, si individuano e si studiano quelli che possono compromettere la realizzazione dei fini aziendali prefissati, non solo da un punto di vista economico - finanziario (guardando ad esempio il rischio di cambio, quello di interesse, ecc.), ma anche da un punto di vista globale dell'azienda, per cui si considera anche l'aspetto qualitativo. Ed è proprio questo l'ambito più delicato, in quanto è molto difficile avere una misura oggettiva di elementi come la "probabilità di deterioramento delle capacità manageriali o della qualità dei servizi prestati"[17].

La sopravvivenza di un sistema aziendale è strettamente legata alla capacità di gestire i rischi interni ed esterni, ed è quindi prerogativa del sistema di controllo provvedere ad identificarne e valutarne la valenza[18], per poter poi definire dei controlli specifici che vadano a fronteggiare ogni possibile situazione creatasi.

Si identificano quindi le fasi di:

16 Beretta S., "Valutazione dei rischi e controllo interno", 2004.
17 Bava, F., *Op. cit.*, 2003.
18 Beretta S., "Valutazione dei rischi e controllo interno", 2004.

- Risk Assessment, ovvero identificazione dei rischi che hanno potenziali ripercussioni sull'attività aziendale;
- Risk Evaluation, nonché la classificazione dei rischi in termini di impatto e probabilità, per poter stabilire le priorità di intervento con i processi di mitigazione.

Combinando queste due variabili il management potrà cogliere i rischi significativi procedendo ad una mappatura dei rischi.

La successiva componente del Framework CoSO è quindi proprio l'attività di controllo che riguarda "l'insieme delle politiche e delle procedure che devono essere attivate per ridurre i rischi connessi al raggiungimento degli obiettivi" [19], garantendo dunque un reale perseguimento delle strategie manageriali.

Possiamo individuare essenzialmente tre categorie di attività di controllo:

- controlli relativi agli aspetti operativi;
- controlli sulle informazioni di bilancio;
- controlli sul rispetto dei vincoli legali e regolamentari.[20]

La quarta componente riguarda l'aspetto legato al flusso informativo, ovvero prevede che le comunicazioni vengano trasmesse in maniera rapida ai soggetti coinvolti affinché questi possano svolgere correttamente i loro compiti. Le comunicazioni seguono quindi le seguenti direzioni:

- verso il basso, cioè nei confronti dei dipendenti
- verso l'alto, cioè dirette al management;
- trasversalmente, attraverso l'intera organizzazione e nei confronti dei vari stakeholders che si relazionano con l'azienda.[21]

Garantire un corretto funzionamento del sistema informativo permette di creare unità e coesione tre le diverse parti aziendali così che si possa diffondere "la cultura del controllo" e queste possano effettuare correttamente le proprie attività, in modo da adottare un continuo adeguamento dei comportamenti aziendali ai cambiamenti del contesto esterno.

Per ultimo, il quinto elemento del Framework CoSO è costituito dal monitoraggio: questa attività si propone di testare nel tempo che i sistemi di controlli interni

[19] Bava, F., *Op. cit.*, 2003.
[20] Venturelli F., *Op. cit.*, 2007.
[21] Bava, F., *Op. cit., 2003.*

adottati siano aggiornati e adeguati a poter affrontare i possibili scenari che si prefiggono nei vari livelli aziendali.

Questa attività di controllo può avvenire sostanzialmente secondo due modalità[22]:

- attività di supervisione continua, che consiste nelle normali attività di verifica, tra cui vi sono le regolari manutenzioni effettuate dal personale;
- valutazioni specifiche, le quali è opportuno che vengano svolte da soggetti altamente specializzati e indipendenti rispetto al sistema di controllo da analizzare; spesso ad avere questa funzione sono i revisori interni, che vanno alla ricerca di eventuali punti di debolezza del sistema e danno dei suggerimenti al management al fine di colmare tali lacune.

Con il modello delineato nel 1992 si va quindi oltre alla singola visione precedentemente discussa sulla mera attività di tipo ispettivo, richiedendo quindi una continua ed efficiente attività di valutazione del rapporto costi/benefici in modo da ottenere una gestione del rischio appropriata così come un'adeguata attività di controllo.

[22] Lisi, P. "*I sistemi di controllo interno in primo piano*", in "A&F" n. 20 del 1998.

1.3 Il framework COBIT: la gestione delle infrastrutture IT

L'ultimo decennio del XX secolo è stato caratterizzato dalla crescita nella maggior parte delle aziende, dell'utilizzo di infrastrutture IT come guida su cui affidarsi per il raggiungimento del successo aziendale.

La necessità di gestire queste infrastrutture ha fatto sì che si abbandonassero i precedenti framework IT di best practice, volti al miglioramento della gestione dei costi e delle risorse attraverso metodi predittivi.

Il COBIT ha fatto sì che le aziende abbiano potuto seguire delle guide linea essenziali per sviluppare, controllare e mantenere i rischi e la sicurezza IT, indipendentemente dal proprio settore di appartenenza.

L'associazione professionale internazionale ISACA ha redatto il COBIT per la prima volte nel 1996, come una serie di obiettivi di controllo per aiutare le società di Audit contabile a poter lavorare meglio nei contesti relativi a strutture IT.

Con il passare del tempo, man mano che il valore e il potenziale di tali attività all'interno dell'auditing diventavano sempre più evidenti, l'ISACA rilasciò una nuova versione più completa nel 1998, ampliando notevolmente il concetto di controllo aggiungendo il framework di gestione.

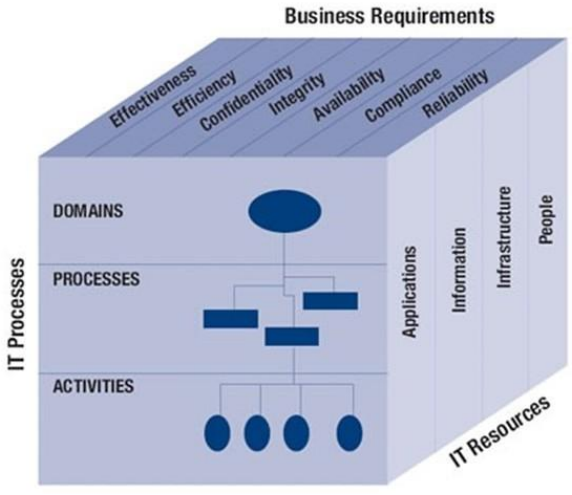


Figura 2 - COBIT cube

Il framework del COBIT crea una struttura a tre livelli, composta da elementi quali i requisiti aziendali (ad esempio metriche di integrità, efficacia, affidabilità e conformità), le risorse IT (tra cui infrastrutture e applicativi) e i processi IT, le cui

associazioni sono indicate tramite una rappresentazione a cubo, visibile nella ***Figura 2***, come già visto con il Framework COSO.

Tutti i processi sono elencati tramite quattro domini:

- OP, pianificazione e organizzazione;
- AI, intelligenza artificiale volta ad acquisizione e implementazione;
- DS, fornitura e supporto;
- ME, Monitoraggio e valutazione.

1.3.1 Specifiche del framework COBIT:

L'orientamento societario verso il framework COBIT prevede:

- il collegamento degli obiettivi aziendali agli obiettivi IT;
- la fornitura di metriche di informazioni e modelli di maturità per l'accertamento del livello dei risultati;
- la notazione delle responsabilità correlate dei proprietari di processi aziendali e IT.

Per comprendere appieno l'ambito delle modalità di funzionamento del framework COBIT, vengono forniti due parametri principali:

- Il controllo, come forma di procedure, pratiche, politiche e strutture organizzative progettate per fornire un livello accettabile di garanzia che gli obiettivi e le strategie aziendali saranno raggiunti e gli incidenti indesiderati verranno rilevati e corretti in modo rapido e conciso.
- L'obiettivo di controllo IT, come una dichiarazione del livello di risultati accettabili da raggiungere implementando procedure di controllo relative a una particolare operazione IT.

Il framework COBIT mira a colmare le distanze che c'erano tra i modelli di controllo aziendali come il COSO, e i controlli più mirati all'ambito IT.

1.3.2 Gli obiettivi e vantaggi apportati

Il concetto di base del framework COBIT è che il controllo nell'IT viene raggiunto concentrandosi sulle informazioni necessarie per supportare gli obiettivi o i requisiti aziendali, e trattando le informazioni come risultato dell'applicazione combinata di risorse correlate all'IT che devono essere gestite da processi IT.

Il COBIT include quindi i seguenti componenti:

- Il framework di riferimento, ovvero l'organizzazione e classificazione degli obiettivi di governance IT e le buone pratiche in base ai domini e ai processi IT prima di associarli ai rispettivi requisiti aziendali.
- La descrizione dei processi, ovvero un modello di riferimento e l'uso di un linguaggio comune per tutti i livelli aziendali.
- Gli obiettivi di controllo, che permettono di utilizzare un set di requisiti ad alto livello per un controllo efficace di ogni processo IT.
- Linee guida per la gestione, al fine di assegnare responsabilità, concordare obiettivi, misurare le prestazioni e illustrare l'interrelazione con altri processi.
- Modelli di maturità, volti a valutare la stessa maturità e capacità del processo di controllo e aiutare ad affrontare e prevenire eventuali lacune.

Questo framework offre quindi modelli che aiutano a massimizzare il valore e la fiducia nell'IT e le linee guida forniscono alle organizzazioni di auditing e alle aziende della consulenza IT un framework più esteso per aiutare a raggiungere e mantenere gli obiettivi e le strategie aziendali.

Mentre il mondo continuava a orientarsi verso un ambiente di diverse tecnologie emergenti, l'informazione e l'IT diventavano sempre più un elemento chiave di successo di molte organizzazioni, ma allo stesso tempo sollevavano altri problemi di gestione e governance impegnativi e complessi per professionisti della sicurezza, leader aziendali e specialisti della governance. Le nuove aziende richiedevano una particolare attenzione e controllo sui nuovi scenari di rischio che si andavano a delineare.

1.4 Dagli scandali finanziari del nuovo millennio alla nascita della nuova normativa

La situazione generale americana, intorno ai primi anni 2000, era caratterizzata dal collasso della bolla speculativa legata al boom delle società tecnologiche e soprattutto da comportamenti da parte di manager insensati e assolutamente privi di scrupoli morali che costantemente amplificavano, in maniera fraudolenta e non veritiera, le prospettive favorevoli della società, occultando alcune criticità gestionali, economiche e finanziarie.

Le stesse regole contabili e di corporate governance venivano considerate solo ed esclusivamente come schemi rigidi, formali da rispettare solo in apparenza: non erano viste come strumenti per garantire la corretta informativa al pubblico degli investitori sui loro investimenti, quindi non garantivano sostanzialmente un'azione di controllo su decisioni di vertice aziendale da parte delle autorità pubbliche.

L'emblematica evidenza di tali anomali meccanismi è rappresentata dal caso Enron, ma a esso seguirono altri collassi contabili, come quelli di Global Crossing (soprattutto a causa della pubblicazione sovente di bilanci pro forma basati su assunzioni e ipotesi e non su ipotesi reali), Adelphia Communications, Tyco International, Xeros Corp, Qwest Communication International, tutti casi in cui si manifestava un'infedele rappresentazione delle situazioni economico, patrimoniali e finanziarie degli attori imprenditoriali coinvolti. Il punto di svolta, è avvenuto nel giugno del 2002, e riguarda il fallimento della società di telecomunicazioni Worldcom, la quale aveva una gestione totalmente determinata da Bernie Ebbers, fondatore e CEO della società, senza la presenza di un sistema bilanciato di poteri relativi alla gestione e di responsabilità. Nei primi anni duemila, la redditività ha cominciato a diminuire e il CEO ha risolto la questione attraverso il falso in bilancio; il suo fallimento, risulta essere uno dei più importanti della storia, dato che viene quantificato in "oltre 103 miliardi di dollari"[23].

I tratti che accomunavano tutti questi scandali, sono quindi rappresentati da gravi irregolarità contabili e governance assolutamente deboli. Della falsità di queste

[23] Confindustria, *Op. cit.*, 2002.

situazioni era al corrente anche il loro revisore, che per molte di esse era rappresentato da Arthur Andersen, il quale invece di far emergere la verità, ha ulteriormente coperto queste pratiche contrarie alla corretta gestione.

Di conseguenza, era necessario riconquistare la fiducia del mercato e tutelare maggiormente i titolari di azioni riguarda le frodi di cui avrebbero potuto essere vittime.

1.4.1 Il caso Enron

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

Il crollo della Enron vede tra le principali cause la dichiarazione di falsi in bilancio certificati dalle società di revisione, prima fra tutte la società Arthur Andersen. I primi sospetti vennero dall'eccessiva quotazione in borsa della Enron e, per questo, lo Stato della California avviò un'inchiesta su presunte manipolazioni del mercato da parte di quest'ultima e di altri rivenditori di energia.

L'inchiesta da parte della Security and Exchange Commission (la corrispondente della CONSOB italiana, nel seguito indicata con l'acronimo SEC), che seguì al tracollo della Enron, non si concentrò solo sulla società energetica ma anche sulla sua società di revisione Arthur Andersen.
Indagando a fondo emerse che la Enron manteneva alto il livello dei redditi utilizzando manipolazioni contabili con l'ausilio dei suoi revisori, i quali confessarono di aver distrutto documenti importanti e per tale motivo l'Arthur Andersen fu accusata di intralcio alla giustizia, e perse, inoltre, la licenza per la certificazione dei bilanci[24].

[24] Masters, 2011

«La Enron ha derubato la banca», dirà il deputato James Greenwood, tra gli inquirenti della commissione governativa, «la Andersen le ha fornito l'auto per scappare, e si è messa al volante».[25]
Eppure, solo l'anno prima il Financial Times, aveva definito la Enron "azienda energetica dell'anno", in seguito ai successi riscontrati nell'attività di intermediazione.
Invece, un anno dopo gli eventi subirono una forte accelerazione fino ad arrivare a dicembre 2001 quando avvenne il tracollo in borsa.

Dal 2001 la Enron cessò di esistere; i danni a investitori, pensionati, comunità e mercati furono storici.

Il tracollo della Enron indusse molti esperti a riflettere sulla gravità dei fatti accaduti e a rilevare i punti deboli e le carenze di tutti i soggetti costituenti il simbolo del sistema capitalistico mondiale, ossia quello americano. La carenza strutturale principale che emerse fu quella della revisione contabile, la quale mostrò non solo una défaillance professionale, ma anche e soprattutto la mancanza di "etica", in quanto furono distrutti documenti importanti per nascondere i fatti. Inoltre, emersero:

- il problema delle società di rating che non avevano segnalato per tempo il degradarsi del merito di credito;

- il problema degli analisti finanziari che avevano continuato a emettere consigli di "buy" o perfino di "strong buy";

- il problema della rappresentazione della realtà aziendale da parte del management;

- infine, le carenze normative sia in tema di controlli interni, che di responsabilità del management, sia delle società di revisione, e del modello di impresa[26].

[25] Leda Balzarotti e Barbara Miccolupi, 2016
[26] Demattè, 2002

Il caso Enron ha "affondato" la società di revisione Arthur Andersen, in quanto la SEC che ha indagato sulla bancarotta di Enron, ha dimostrato che alcuni manager della Andersen hanno distrutto una mole ingente di documenti connessi al caso in oggetto, ma ancor peggio hanno certificato una situazione contabile e di bilancio assolutamente non corrispondente al vero, ignorando perdite per oltre 1 miliardo di euro.

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.

1.4.2 La normativa SOX e il ruolo della PCAOB

Il "Caso Enron" ebbe risonanza internazionale ed indusse le autorità americane ad intervenire in modo tempestivo e incisivo affinché non si ripetessero casi simili.
Per ripristinare la fiducia dell'opinione pubblica nell'affidabilità della rendicontazione finanziaria, il Senato e la Camera dei rappresentanti degli Stati Uniti approvarono il Sarbanes-Oxley Act del 2002 (Pub.L. 107-204, 116 Stat. 745, 30 Luglio 2002).

La Sarbanes-Oxley Act, conosciuta anche con il nome di "Public Company Accounting Reform and Investor Protection Act of 2002" e comunemente chiamata Sarbanes-Oxley, Sarbox (o semplicemente SOX)[27], è una legge federale emanata nel luglio 2002 dal governo degli Stati Uniti d'America. Si trattava, in origine, di due diversi disegni di legge proposti dal deputato Mike Oxley (repubblicano, eletto nell'Ohio) e dal senatore Paul Sarbanes (democratico eletto nel Maryland): i due disegni furono unificati da una commissione bicamerale nell'atto finale approvato il 24 luglio 2002 con grandissima maggioranza in entrambe le camere, e firmato dal presidente George W. Bush il 30 luglio.

[27] Wikipedia, *"l'enciclopedia libera.", 2017*

La legge mirava a chiudere alcuni "buchi" o "falle" nella legislazione americana, al fine di migliorare la corporate governance delle aziende e garantire la trasparenza delle scritture contabili, agendo tuttavia anche dal lato penale, con l'incremento della pena nei casi di falso in bilancio e simili. Venne, inoltre, aumentata la responsabilità degli auditor all'atto della revisione contabile.

Secondo alcuni storici dell'economia, si tratta di uno degli atti governativi più significativi in campo economico dai tempi del New Deal[28].
I punti su cui la legge focalizzò la sua attenzione furono:

- maggiore responsabilità per il management per quanto concerne l'accuratezza delle informazioni contabili sui bilanci e relazioni finanziarie;
- venne creata una nuova autorità di controllo sui revisori esterni;
- vennero aumentate le pene per i crimini contabili e illeciti fiscali.

La normativa SOX, tuttora in vigore, introdusse nuove procedure per le verifiche contabili ed inoltre stabilì che tutte le aziende pubbliche che avevano dei titoli nella borsa americana avrebbero dovuto soddisfare i requisiti espressi dalla legge.
Venne quindi istituito il "Public Accounting Oversight Board" (di seguito PCAOB), ovvero il consiglio di vigilanza sui bilanci delle aziende quotate[29].
Al Board venne affidato il compito di regolamentare le seguenti attività:

- auditing e i relativi standard di attestazione, di controllo della qualità delle procedure che le società di revisione avrebbero dovuto seguire nell'emissione dei report;
- i comportamenti da seguire qualora fosse stato necessario intervenire in modo appropriato, per proteggere gli interessi degli investitori.

In definitiva, le nuove norme miravano, da un lato, ad obbligare le aziende ad implementare un effettivo sistema di controllo interno, dall'altro, a responsabilizzare i revisori attraverso la definizione di standard professionali

[28] Con New Deal si intende il Programma di politica economica attuato negli Stati Uniti dal neoeletto presidente F.D. Roosevelt fra il 1933 e il 1939 per porre rimedio ai disastrosi effetti della grande crisi che tra il 1929 e il 1932 aveva investito dapprima il sistema capitalistico statunitense per estendersi poi rapidamente anche in Europa.
(*versione online dell'enciclopedia Treccani*).
[29] Public Accounting Oversight Board" (PCAOB), *sito ufficiale "https://pcaobus.org "*

maggiori, pur garantendone l'indipendenza. In definitiva il PCAOB ha come obiettivo il miglioramento della qualità della revisione mediante un frequente controllo sull'operato delle società di revisione, e qualora fosse necessario, anche attraverso l'imposizione di sanzioni.

Il Sarbanes-Oxley Act non impose, direttamente, i requisiti per la sicurezza dei dati aziendali, ma conteneva tutta una serie di clausole riguardanti il controllo interno, la completezza della documentazione aziendale sensibile e lo stato delle verifiche contabili.

Di seguito sono sintetizzate le caratteristiche principali della struttura del PCAOB e le corrispettive funzioni da essa assunta nei confronti delle governance e degli organi di controllo interno societari.[30]

L'atto stabilisce in primis che il PCAOB, avente sede in Washington DC, è un organismo non a scopo di lucro, che è composto da cinque membri, i quali vengono scelti dalla SEC con un incarico di durata a tempo pieno per 5 anni e due di loro devono essere CPA.

L'organismo della SEC deve approvare a riguardo del PCAOB il budget annuale e le regolamentazioni proposte, includendo gli standard di revisione.

Il Sarbanes-Oxley Act ha definito le funzioni del PCAOB che includono[31]:

- il Registro delle Società di Revisione che stabilisce gli standard di revisione, etica, controllo della qualità, indipendenza e preparazione dei rapporti;
- il miglioramento della qualità delle revisioni medianti ispezioni ad hoc sulle società stesse;
- l'indagine sull'operato dei revisori imponendo eventuali sanzioni contro le società di revisione e le persone associate alle medesime.

"La PCAOB ha il compito di migliorare la qualità della revisione"[32] attuando ispezioni di controllo con cadenza annuale in caso di società di revisione che hanno il più grande numero di incarichi, mentre ogni tre anni per tutte le altre.

[30] Migliavacca, Cadeddu, Porcelli*; Orientamenti Internazionali su Governance e Controllo Interno – SARBOX ACT, 2014*

[31] Migliavacca, 2014

[32] Migliavacca, Cadeddu, Porcelli*; Orientamenti Internazionali su Governance e Controllo Interno – SARBOX ACT, 2014*

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.

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

In particolare, le società quotate al NYSE sono interessate principalmente alle sezioni, visibili nella ***Figura 3,*** che sono:

- Responsabilità Societaria (Corporate Responsability) – Section 302, 906
- Miglioramenti dell'informativa finanziaria – Section 404

Figura 3 Sezioni SOX

La "sezione 302" richiede che il funzionario o i funzionari esecutivi principali di una società, il responsabile o i responsabili finanziari principali certifichino personalmente di essere responsabili dei controlli e delle procedure di divulgazione per ciascuna relazione trimestrale o annuale. Per la maggior parte delle aziende, i funzionari di certificazione sono il CEO e il CFO.

La novità introdotta da questa sezione è proprio l'imposizione, in capo a questi ultimi, di un obbligo di certificazione dei bilanci che attesti che hanno effettuato una valutazione della progettazione e dell'efficacia di tali controlli al fine di

migliorare l'informativa finanziaria. A maggiore supporto di tale obiettivo, i responsabili della certificazione devono dichiarare di aver comunicato al loro comitato di revisione contabile e al revisore indipendente eventuali carenze significative nei controlli, debolezze rilevanti e atti di frode. La SEC ha inoltre proposto un requisito di certificazione ampliato che include i controlli interni e le procedure per l'informativa finanziaria, oltre al requisito relativo ai controlli e alle procedure di divulgazione.

Analizzando più nel dettaglio i ruoli, Il CEO deve ora riconoscere direttamente la responsabilità del controllo interno che in precedenza era stato in gran parte delegato al CFO. Ad ogni presentazione trimestrale e annuale, il CEO e il CFO devono certificare che:

- sono responsabili dei controlli e delle procedure di comunicazione;
- hanno progettato (o supervisionato la progettazione di tali controlli) al fine di assicurare che le informazioni rilevanti siano loro rese note;
- hanno valutato l'efficacia di tali controlli con cadenza trimestrale;
- hanno presentato le loro conclusioni in merito all'efficacia di tali controlli;
- hanno comunicato al loro comitato per il controllo interno e alla società di revisione contabile eventuali carenze significative dei controlli, carenze rilevanti e frodi che coinvolgono il management o altri dipendenti che hanno un ruolo determinante nel controllo interno della società;
- hanno indicato nel deposito eventuali modifiche significative dei controlli.[33]

La certificazione dell'articolo 906 è una dichiarazione più breve, in cui è richiesto al CEO e ai CFO di firmare e certificare la relazione periodica contenente i rendiconti finanziari. La suddetta certificazione esecutiva deve affermare che la relazione è conforme ai requisiti di reporting della SEC e rappresentare correttamente la condizione finanziaria dell'azienda e i risultati delle sue operazioni. Il mancato rispetto di questo requisito comporta multe fino a 5 milioni

[33] *SOX Section 302: Corporate Responsibility for Financial Reports*, Sarbanes Oxley, https://www.sarbanes-oxley-101.com/SOX-302.htm

di dollari e può essere imposta la reclusione fino a 20 anni per non conformità consapevole o intenzionale.[34]

L'aspetto innovativo introdotto dalla sezione 404 è la dichiarazione da parte del CFO e del CEO dell'esistenza e adeguatezza dei controlli interni sul bilancio e sulle ulteriori informazioni finanziarie pubbliche.

La sezione 404 obbliga, infatti, le società a includere nella loro relazione annuale un rapporto di controllo interno del management che:

- afferma di essere responsabile dell'istituzione e del mantenimento dei controlli interni e delle procedure di informativa finanziaria;
- valuta e giunge a conclusioni sull'efficacia dei controlli interni e delle procedure di informativa finanziaria;
- dichiara che la società di revisione contabile ha attestato e riferito in merito alla valutazione, da parte del management, dei controlli interni e delle procedure di informativa finanziaria della società, seguendo gli standard istituiti dal PCAOB. [35]

Gli auditor esterni devono attestare, redigendo una relazione separata, l'efficacia del controllo interno della società e l'affermazione del management sull'efficacia dei controlli interni e delle procedure per l'informativa finanziaria. Il rapporto da redigere deve contenere[36]:

- Dettagli su come il management gestisce e mantiene un adeguato sistema di controllo interno sulla rendicontazione finanziaria supportato da idonee evidenze.
- Dettagli sul framework, che deve essere un modello di controllo idoneo e riconosciuto, utilizzato dal management per la valutazione dei controlli interni, al fine di fornire criteri ai valutatori sull'efficacia del sistema.

[34] *SOX Section 906: Corporate Responsibility for Financial Reports*, Sarbanes Oxley, https://www.sarbanes-oxley-101.com/SOX-906.htm
[35] *SOX Section 404: Management Assessment of Internal Controls*, Sarbanes Oxley, https://www.sarbanes-oxley-101.com/SOX-404.htm
[36] *SOX Compliance Requirement & Overview*, 15 Gennaio 2020, AUDITBOARD, https://www.auditboard.com/sox-compliance/

- Descrizione completa degli obiettivi di controllo creati dal management per affrontare i rischi identificati e le relative attività di controllo.
- Descrizione dei sistemi informativi e delle procedure di comunicazione in atto a supporto di quanto sopra.
- Valutazione a fine anno da parte del management dell'efficacia del sistema di controllo interno comprensivo di ogni material weakness identificata, con attestazione ulteriore da parte del revisore indipendente dalla società sulla valutazione del controllo interno sulla rendicontazione finanziaria.
- Descrizione del processo di comunicazione alla società di revisione e al comitato per il controllo interno delle carenze significative e delle debolezze rilevanti.
- Descrizione delle procedure di monitoraggio per assicurare che la struttura di controllo interno funzioni come previsto e che i risultati delle procedure di monitoraggio siano esaminati e seguiti.

La SEC impone la divulgazione al pubblico di qualsiasi material weakness identificata nel sistema di controllo interno. Il controllo interno è ritenuto efficace se rientra in determinate soglie, ovvero non ha debolezze sostanziali nel design e nell'operation.

Le condizioni da segnalare sono carenze di controllo che vengono sottoposte all'attenzione del revisore indipendente e che, a suo giudizio, dovrebbero essere comunicate al comitato di revisione perché rappresentano carenze significative nella progettazione o nel funzionamento del controllo interno, che potrebbero influenzare negativamente la capacità dell'organizzazione di avviare, registrare, elaborare, riassumere e riferire dati finanziari e non finanziari accurati.

1.5 La risposta italiana alla normativa SOX

L'adeguamento alla SOX è richiesto alle società italiane quotate in USA oppure alle società che sono controllate da gruppi quotati in USA. Il legislatore italiano è stato di conseguenza indotto a inserire una nuova normativa nella legislazione

nazionale, la Legge sul risparmio, (legge 28 dicembre 2005, n. 262) con l'intento di migliorare l'informativa finanziaria delle società quotate.

Detta Legge, dal titolo significativo "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari", ha profondamente modificato il D.lgs. 24 febbraio 1998, n. 58 denominato Testo Unico della Finanza, introdotto in applicazione degli artt. 8 e 21 della Legge 6 febbraio 1996, n. 52.

In particolare, l'articolo 154-bis, il primo della sezione V bis del D.lgs. n. 58/98 TUF, tratta sulla redazione dei documenti contabili societari e prevede la nomina di un dirigente, scelto dall'organo di controllo aziendale, che è preposto alla redazione degli stessi. Egli ha il compito di scrivere una dichiarazione, insieme al direttore generale, che attesti sulla veridicità della situazione economica, patrimoniale e finanziaria della società al fine di certificare gli atti e le comunicazioni diffuse sul mercato e previste dalla legge[37].

In realtà detto articolo, così come si trova nella sua stesura odierna, fu dapprima modificato dall'art. 14 della Legge n. 262 del 28/12/2005 e successivamente dall'art. 3 del D.lgs. n 303 del 29/12/2006 e dall'art. 1 del D. Lgs. n. 195 del 6/11/2007. Il tutto sta a dimostrare la continua evoluzione della materia e la volontà del legislatore di offrire strumenti normativi sempre più adeguati alle esigenze del settore.

Ovviamente le continue modifiche rischiano di "appesantire" il settore, poiché si rischia di cercare di coprire ogni possibile aspetto della materia rendendo le nomine e i controlli societari eccessivamente farraginosi.

Il dirigente preposto deve anche predisporre procedure amministrative e contabili per ogni comunicazione di carattere finanziario e per la redazione del bilancio d'esercizio e del bilancio consolidato. Ne deriva che, al fine di rispettare questi

[37] Art. 154-bis Dirigente preposto alla redazione dei documenti contabili societari, TUF 16 marzo 2018, RicercaGiuridica.com,
https://www.ricercagiuridica.com/codici/vis.php?num=24786&search=

compiti assegnatigli, il preposto deve avere adeguati poteri e mezzi per ricavare le informazioni.[38]

L'articolo prevede infine la scrittura da parte degli organi amministrativi delegati e del dirigente preposto di una relazione che attesti la corrispondenza del bilancio alle risultanze documentali, delle scritture e dei libri contabili, da allegare al bilancio d'esercizio e a quello consolidato, se previsto.

La normativa introduce la responsabilità, anche penale, dei dirigenti preposti alla redazione dei documenti contabili societari, al pari degli amministratori, in base ai compiti svolti, salve le azioni esercitabili in base al rapporto di lavoro con la società. Il dirigente preposto può infatti essere soggetto al reato di false comunicazioni sociali e al reato di ostacolare le Autorità pubbliche di vigilanza nelle loro funzioni.

La legge 262 è stata introdotta a completamento del decreto legislativo 231 del 2001 che ha introdotto la responsabilità amministrativa degli enti per reati commessi da soggetti appartenenti ad essi. Il Dlgs. 231 secondo quanto pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 2001, si applica alle società, alle associazioni e agli enti dotati di personalità giuridica e non, ad esclusione degli enti pubblici che svolgono funzioni di rilievo costituzionale.

Le persone considerate sono coloro che svolgono funzioni di rappresentanza, di direzione, di amministrazione, coloro che esercitano la gestione e il controllo anche di fatto o persone sottoposte alla vigilanza o alla direzione di uno di loro. L'ente è esonerato dalla responsabilità se l'organo dirigente ha adottato modelli di gestione e di organizzazione idonei a prevenire i reati, non trascurando di applicare un'attenta vigilanza.

La legge richiede che per attuare in modo efficace un modello di organizzazione, vi sia un sistema sanzionatorio idoneo per il mancato rispetto delle misure, ma

[38] Natale Prampolini, *La legge 262/05 e le sue implicazioni, 2011, AIEA*

anche una verifica periodica di esso affinché sia sempre allineato ad eventuali mutamenti dell'organizzazione[39].

1.6 Controllore e controllato: la revisione esterna

La comparsa della revisione esterna avviene a seguito del sorgere della necessità, tra azionisti delle varie società, di avere una verifica, effettuata da un'entità indipendente, se quanto riportato nel bilancio contabile corrispondesse al vero.

Avere un sistema di controllo interno effettuato dalle stesse risorse dell'entità controllata non è sufficiente a garantire a fornire un'opinione sui rendiconti finanziari rappresentate correttamente secondo i principi contabili, poiché si possono generare spesso problemi sul monitoraggio e di incentivazioni riguardo certe informazioni contabili che possono essere manipolate e modificate ad hoc per scopi specifici e diversi da quelli effettivi del controllo. Un controllo effettuato esclusivamente in maniera interna potrebbe incentivare i manager a mentire o a condurre controlli in maniera fraudolenta, che non rispecchiano le vere prospettive societarie come ad esempio operazioni di occultazione di criticità gestionali e finanziare oppure falsificando direttamente i dati di bilancio.

Per tutte queste ragioni il ruolo del controllore e del controllato non possono sussistere solo all'interno della stessa organizzazione, quindi si deve ricorrere ad una società di revisione che eroghi un servizio definito attraverso un rapporto di agenzia.

Trattandosi di società in scopo SOX sotto controllo ICFR, queste hanno il dovere di stipulare un contratto, definito da un adeguato sistema di incentivi, con una società di consulenza esterna che revisioni le attività svolte dal loro sistema di controllo interno. Nonostante ciò resta però il problema su chi controlla l'operata dell'attività del controllore esterno.

[39] Decreto Legislativo 8 giugno 2001, n. *231, pubblicato nella* Gazzetta Ufficiale *n. 140 del 19 giugno 2001*

A tal ragione, a seguito degli scandali Enron e Worldcom, è stato istituito il PCAOB, una società non a scopo di lucro con lo scopo di tutelare gli azionisti da possibili attività illecite svolte nell'operato delle società di revisione, sorvegliando attraverso specifiche attività di controllo l'applicazione degli adeguati principi contabili SOX.

In conclusione, per agire in conformità con i principi normativi precedentemente espressi, le varie aziende hanno la necessità di dover disporre di un framework di riferimento e di una governance adeguata ad affrontare i rischi etici. In questo modo le società possono garantire una corretta gestione ai propri partner e soci azionisti senza dover affrontare le azioni normative, multe e perdite di reputazione che si verificherebbero in assenza del controllo.[40]

[40] PWC Israel, *Compliance,* https://www.pwc.com/il/en/Advisory/compliance.html

Capitolo 2

2.1 I sistemi IT e il ruolo dell'auditor esterno

La rendicontazione contabile per le aziende assume un ruolo chiave per offrire informazioni esaustive e complete sulla gestione agli utilizzatori stessi e a tutti coloro che in qualche modo sono interessati ad esso. Devono quindi essere rispettati dei principi fondamentali per assicurare:

- La chiarezza, ovvero che il bilancio risulti comprensibile e trasparente per gli stakeholders;
- La veridicità delle informazioni, ovvero in termini di espressioni di quantità oggettive veritiere e stime attendibili.
- La correttezza, ovvero l'applicazione di principi contabili, normative e regole amministrative.

A seguito dell'incremento di complessità di processi aziendali e delle moli di informazioni contabili da dover registrare, già a partire dagli anni Sessanta, si sono iniziati ad utilizzare i sistemi informativi, con lo scopo di supportare la rendicontazione finanziaria e contabile per garantire una maggiore correttezza e rapidità di calcolo.

Con il tempo il sistema contabile si è trasformato da solo raccoglitore ed elaboratore di dati di natura contabile ed economica a polmone informativo principale di tutta l'azienda.[41]

Il sistema informativo contabile è definito non solo dai dati elementari che in aggregato lo costituiscono, ma anche da elaborazioni contabili e statistiche che permettono all'azienda di determinare il patrimonio finanziario, i risultati di esercizio e documentare ai fini fiscali le dichiarazioni presentate. Inoltre, l'utilizzo dei sistemi informativi giova a favore delle aziende come supporto alle decisioni aziendali imprenditoriali e di monitoraggio delle attività.

[41] U. Bertini, Il sistema d'azienda, Giappichelli, Torino, 1990

Col tempo quindi il sistema informativo aziendale ha assunto un ruolo fondamentale per la gestione della contabilità del personale, del magazzino e industriale, ai fini di effettuare analisi e controllo dei costi.

L'efficacia dell'utilizzo dei sistemi informativi è stata permessa quindi dall'automazione intrinseca nei processi aziendali, permettendo quindi di potenziare la capacità di informazioni dei dati contabili consentendo di gestire ed effettuare elaborazioni contabili su moli di dati che sarebbero impossibili da trattare in maniera manuale.

Tuttavia, i vantaggi che possono essere espressi da questo processo sono strettamente legati alla correttezza e accuratezza che viene utilizzata nel processo di immissione dei dati nel sistema informativo, e alle procedure di gestione ed elaborazione dello stesso: nasce da qui la necessità di avere all'interno delle aziende un processo di supporto per la valutazione e la gestione dei rischi che sono intrinseci nei sistemi informativi.

2.1.1 Il rischio IT

Il rischio IT è un rischio che appare come direttamente legato al malfunzionamento dei sistemi informativi, così come indirettamente alle conseguenze che potrebbe avere sui processi operativi aziendali: è definito come il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologie nei sistemi informativi.

Data l'importanza dell'accuratezza informativa societaria, come già anticipato nel precedente capito, dei numerosi scandali finanziari che hanno colpito i primi anni duemila, sono state introdotte una serie di normative, a partire dalla SOX, per mitigare e gestire il rischio IT. Le nuove disposizioni hanno fatto si, che all'interno del controllo interno aziendale, abbia preso piede una sotto parte dedicata all'audit IT, ovvero un processo di verifica sistematico e documentato, condotto da personale esperto e imparziale, con il compito di tutelare l'azienda dai rischi ICT.

Questo comporta che siano applicati protocolli di efficienza e sicurezza per i processi di supervisione IT, che hanno il compito in primo luogo di fornire un ambiente sicuro e ben controllato per migliorare le prestazioni aziendali e, in secondo luogo, di assistere l'organizzazione per affrontare in maniera strategica i requisiti di governance, rischio e conformità.[42]

In termini di conformità è divenuto essenziale la capacità di mantenere e proteggere le informazioni, per garantire:

- una corretta applicazione e rispetto delle regole interne, delle norme e delle best practice definite;
- e di seguire le leggi, linee guida e regolamenti imposti da governi, industrie e organizzazioni esterne.[43]

Tra varie definizioni elaborate per il rischio IT viene di seguito riportata quella dell'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)"[44].

Diviene quindi fondamentale il ruolo del management nel dedicare particolare attenzione alla gestione dei sistemi informativi per controllare i potenziali rischi IT che potrebbero portare a ingenti perdite economiche e gravi conseguenze reputazionali.

I rischi IT dipendono sia dalla ambiente del settore in cui l'organizzazione opera, sia dal tipo di configurazione dei sistemi informativi così come da vari fattori

[42] Technology risk, PWC, Australia, https://www.pwc.com.au/risk-controls/technology-risk.html

[43] Smartsheet, *Maintain, Protect, and Diminish Risk with a Comprehensive IT Compliance Strategy*, https://www.smartsheet.com/understanding-it-compliance

[44] The Risk IT Framework, ISACA, USA, 2009

interni ed esterni all'azienda. Tuttavia, molti rischi possono essere accomunati prescindendo dalla loro natura, distinguendosi in:

- Rischio di selezione: ovvero quando la 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: se in un momento di necessità il sistema risulta indisponibile, questo 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.

L'attività di supporto Audit IT svolge quindi un importante ruolo nel segnalare le inadeguatezze dei processi informativi, così che le aziende possano ottenere performance migliori, adeguandosi ai requisiti di rischio, governance e conformità delle normative.

2.2 L'attività di supporto Audit IT

L'auditing è un'attività di verifica di un processo o sistema di qualità, per garantire la conformità ai requisiti normativi; si tratta di attività che richiedono molto tempo poiché spesso sono riferite all'analisi di un'intera organizzazione aziendale.

Nello specifico l'attività di audit IT fornisce un supporto all'audit erogando un servizio che si incentra sull'Information Technology, garantendo informazione ausiliari all'organizzazione per la gestione dei rischi, aiutando le risorse dell'IT nel raggiungere gli obiettivi aziendali.

Proprio mediante la valutazione dei rischi connessi alla gestione dei sistemi IT, l'auditor fornisce valutazioni di adeguatezza e robustezza dei sistemi informativi a supporto dei processi fiscali e contabili, con lo scopo di apportare un continuo miglioramento del sistema.[45]

Data la complessità del rischio IT questo potrebbe essere trasferito a terzi tramite contratti di fornitura esterna; è quindi fondamentale trattare tale rischio in una visione strategica e controllare in maniera accurata il sistema informativo.

A tal scopo è necessaria una collaborazione tra le varie funzioni e le strutture di business al fine di sensibilizzare un corretto impiego della tecnologia dato il rischio cui è legata.

La funzione dell'auditor esterno interviene quindi con il compito di[46]:

- Assistere nel potenziamento dei quadri organizzativi di sicurezza per garantire la conformità agli standard e ai quadri normativi stabiliti
- Allineare il modo in cui la sicurezza viene gestita al quadro di rischio e di controllo dell'organizzazione
- Portare le più recenti conoscenze ed esperienze globali.

[45] IS Audit & Compliance Support, https://www.bdo.it/it-it/services-it/advisory/digital-consulting/is-audit-compliance-support
[46] Technology risk, PWC, Australia, https://www.pwc.com.au/risk-controls/technology-risk.html

Le attività dell'IT audit costituiscono quindi un sottoinsieme di quelle complessive della revisione contabile del bilancio e sono declinate seguendo la natura a cui queste ultime si uniformano.

Difatti, l'attività dell'audit IT è quindi anche guidata dalla necessità di dimostrare la conformità a standard, regolamenti e requisiti imposti esternamente al tipo di organizzazione, settore o ambiente operativo, ed è secondo queste ultime voci che l'auditor pianifica e definisce il sistema di controllo da adottare.

2.2.1 La fase di pianificazione dell'audit IT

Occorre che le attività del processo di Audit IT siano adeguatamente pianificate per garantire l'efficacia del sistema di controllo; seguire un modello di riferimento è di vitale importanza perché permette di:

- Individuare gli obiettivi che l'audit IT intende perseguire, espressi nella fase di valutazione preliminare dei rischi;
- Programmare il workflow operativo in modo da identificare le risorse umane e informatiche che saranno impiegate nell'esecuzione dell'attività;
- Definire una stima delle risorse umane, finanziare e informatiche così come la durata del processo necessaria allo svolgimento dell'attività.

In un primo momento, la pianificazione viene effettuata singolarmente dai revisori contabili i quali si interfacciano con le società clienti per effettuare un'analisi dei processi utilizzati al fine della gestione dei bilanci e della rendicontazione finanziaria. È con questa fase che sono quindi individuate le "significant class of transactions" (SCOTs), nonché le principali voci di bilancio che influisco sulla gestione dei conti societari.

A seguito della definizione delle SCOTs, il team di revisione insieme all'auditor IT identificano congiuntamente quali sono gli applicativi da inserire in perimetro significativi ai fini dell'analisi di rendicontazione finanziaria. In questa fase di pianificazione il team di Audit IT si impegna quindi nell'ottenere informazioni

riguardo le documentazioni e gli aspetti fondamentali per la pianificazione della revisione dei sistemi informativi.

2.2.2 Understanding of IT Enviroment

Il primo documento utile che viene redatto dal team di Audit IT è un'analisi che definisce, all'interno dell'ambiente IT, quali sono le politiche e procedure adottate da un ente societario in termini di infrastrutture informatiche utilizzate per supportare tutti i processi legati alle operazioni di business e definire le strategie finanziarie.

Le attività rilevanti che vengono definite in più sezioni all'intero di questo documento, a seguito di un incontro con il cliente da revisionare, sono:

- Analisi dell'organizzazione attuale dell'area ICT per la definizione delle performance dei servizi implementati in termini di efficacia ed efficienza della stessa funzione;
- Valutazione degli ambienti IT utilizzati per intercettare possibili cambiamenti;
- Identificazione dei principali progetti approvati in ambito ICT per comprendere gli eventuali impatti che possono essere generati sull'ambiente IT analizzando le possibili criticità generatosi.

Queste attività sono tutte rilevate ai fini di poter effettuare una completa mappatura dell'ambiente IT dell'azienda cliente, raccogliendo le informazioni utili al revisore per la comprensione dei rischi connessi ad esso, e permettendo di avere una stima delle tempistiche necessari all'attività di supporto IT.

2.2.3 Risk Assessment

La fase successiva nella pianificazione delle attività di auditing è quella del risk assessment che viene definito come l'analisi e valutazione dei rischi che si evincono da una corretta analisi dell'ambiente e dell'organizzazione IT della società al fine di poter rilevare le criticità che potrebbero intaccare la sicurezza delle informazioni.

In questa fase sono definite le possibili misure che saranno adottate per limitare il rischio e renderlo accettabile sotto una determinata soglia di confidenza.

Uno degli approcci che può essere utilizzato per la realizzazione di un progetto di audit IT è il così detto risk-based approach, che definisce i passaggi:

- analisi e classificazione dei sistemi informativi utilizzati dall'azienda;
- definizioni dei possibili applicativi che impattano sulle funzioni e risorse critiche per il processo di analisi contabile;
- valutazione dei rischi che incidono su questi sistemi e l'impatto che questi hanno sulle funzioni di business;
- infine, identificazione dei controlli appropriati per indirizzare i rischi IT e, sulla base del processo, definizione della frequenza dei controlli.

In particolare, il rischio associato al controllo viene successivamente definito in base ai seguenti fattori associati:

- La natura e la rilevanza degli errori che il controllo intende prevenire o rilevare;
- Se ci sono stati cambiamenti, rispetto agli anni precedenti, nel volume o nella natura delle transazioni che potrebbero influenzare negativamente il controllo e l'efficacia operativa;
- La natura del controllo e la frequenza con cui opera;
- Il grado con cui il controllo si basa sull'efficacia di altri controlli;
- 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;

- In ultimo, se il controllo si basa sulla prestazione di un individuo o è automatizzato (PCAOB, 2007)[47].

La gestione di questi rischi è un requisito fondamentale per i sistemi IT utilizzati dalle società in cui la sicurezza dell'ambiente è un attributo cruciale.

Come indicato dall'ISACA, l'attività di controllo di audit IT consiste nel verificare se qualcuno degli obiettivi di sicurezza di una qualsiasi organizzazione, definiti come "la riservatezza, l'integrità e la disponibilità dei dati", sono rispettati o violati. A tal scopo è necessario tenere sempre presente se qualcuno di questi viene meno durante l'attività di analisi e in quali circostanze specifiche.

La valutazione dei rischi racchiude quindi una serie di procedure sistematiche che possono essere sintetizzate da:

- Identificazione dei danni che derivano da una possibile errore sulla sicurezza dei dati;
- Definizione di una stima delle probabilità di accadimento per un certo evento dannoso, al fine di poter prevedere le possibili vulnerabilità dei controlli attualmente implementati.

Sempre all'interno della fase di pianificazione occorre analizzare come il management dell'azienda abbia adottato pratiche per la gestione dei rischi, per comprendere quali sono le minacce identificate, l'impatto che queste potrebbero aver avuto sull'organizzazione e le misure che sono state applicate eventualmente per affrontarle e mitigarle.

Al fine di avere un supporto durante la fase di risk-assessment possono essere seguiti dei framework che valgono come linee guida per la valutazione. L'utilizzo della matrice dei rischi-controlli ne è un esempio pratico, poiché, sulla base al contesto organizzativo della azienda cliente, contiene l'elenco dei rischi identificati ed i controlli associati, con la loro relativa frequenza, che sono applicati per mitigarli.

[47] 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

In alcuni casi però l'impiego di questi framework non è sufficiente a garantire il successo della fase di valutazione perché è possibile che sia necessario includere dei nuovi rischi rispetto a quelli compresi nella matrice, oppure di dovere modificare dei controlli adattandoli a come vengono gestiti determinati processi nella società in analisi.

2.3 Framework ISO 27001

Al fine di definire uno standard per la sicurezza informatica, nell'ottobre del 2005 viene redatta la normativa internazionale della ISO 27001 che contiene i requisiti per poter gestire la sicurezza dei sistemi informativi, spesso indicata anche come ISMS (ovvero Information Security Management System).

Come l'importanza della governance definita nella sezione 404 della normativa SOX, e così come il framework COSO sulla gestione dei rischi, la gestione della sicurezza delle informazioni è un argomento ampiamente discusso nei vari rami di un'organizzazione.

Lo scopo della ISO 27001 è infatti quello di costituire uno schema completo per le aziende in modo da garantire una corretta gestione della sicurezza della tecnologia dell'informazione adottata all'interno dell'organizzazione.

L'ISMS può essere definito come il framework attraverso il quale il management di una società identifica, valuta e affronta i rischi informativi che sussistono all'interno del sistema. Uno dei punti chiave dello standard è quello di garantire che tutte le disposizioni che vengono prese in materia di sicurezza siano costantemente allineate e ottimizzate con le modifiche alle minacce alla sicurezza, alla vulnerabilità e sugli impatti dell'azienda, poiché questi aspetti hanno assunto un tono sempre più dinamico nel corso dell'ultimo decennio.

Questa normativa ad ogni modo non impone una serie di controlli formali da applicare in tema di sicurezza dei sistemi informativi poiché come già visto in precedenza con l'analisi del rischio i controlli richiesti variano notevolmente a seconda della natura dell'organizzazione che adotta lo standard.

L'ISO 27001 fornisce quindi un'ampia gamma di controlli di sicurezza dell'informazioni, elencati più nello specifico all'interno dell'allegato A della normativa.

Le società che decidono quindi di adottare questo standard sono libere di scegliere qualsiasi siano i controlli di sicurezza da meglio applicare al fine di mitigare i rischi informativi potendo attingere da quelli elencati dal "menù" della ISO 27001 o con la possibilità di integrarli con altri specifici per il proprio contesto.

La chiave per scegliere quali controlli sono applicabili sarà quindi sempre quella di effettuare una corretta e completa valutazione dei rischi informativi dell'organizzazione, che è essa stessa una parte cruciale all'interno dell'ISMS.

Inoltre, l'amministrazione delle società può avere la libertà di scegliere di evitare, condividere o accettare i rischi piuttosto che mitigarli attraverso i controlli, attuando una gestione operativa del rischio all'interno del processo informativo in cui esso stesso è identificato.

Le best practice indicate dalla ISO 27001 possono essere formalizzate secondo due scopi distinti:

- esporre il progetto di un ISMS, definendo le parti importanti ad un livello abbastanza elevato;
- essere utilizzate facoltativamente come base per effettuare una valutazione formale della conformità da parte di revisori al fine di certificare una certa organizzazione (a tal scopo sarà necessaria una serie di documenti obbligatori elencati all'interno della specifica normativa).

La conformità di un'organizzazione alla ISO 27001 è un requisito del tutto facoltativo, ma continua a essere sempre più richiesta ai fornitori e partner commerciali di un'organizzazione al fine di tutelare le loro informazioni e i rischi informativi che possono sopraggiungere lungo tutta la catena di approvvigionamento.

Tra i vantaggi che porta ottenere la conformità a questa normativa vi è sicuramente il riflesso sull'immagine che assume l'organizzazione in termini di qualità e sicurezza. La valutazione infatti richiede di per sé una decisione formale

nel processo di implementazione (implica miglioramenti alla sicurezza e i vantaggi in termini di riduzione del rischio), e richiede in maniera imprescindibile l'approvazione da parte del senior management che porta vantaggio in termini di consapevolezza della sicurezza stessa.

2.4 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 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.

Nell'effettuare un ciclo di audit IT vengono quindi effettuati diverse tipologie di controlli che distinguiamo in:

- ITGC (IT General Controls), ovvero dei controlli volti a verificare se le politiche e procedure aziendali siano correttamente rispettate;

- I controlli applicativi (ITAC), cioè dei controlli automatici eseguiti dai sistemi applicativi delle Società che non richiedono un intervento manuale per la loro esecuzione;
- Infine, i controlli IT dependent manual controls (ITDM) dei controlli che hanno sia una componente automatica che una manuale.

Relativamente ai controlli ITDM vengono effettuati test sulle IPE (Information Produced by Entity) che sono definite come delle informazioni prodotte dalla Società sotto forma di liste, report o tabelle. Queste vengono utilizzate all'interno dei controlli semiautomatici, perciò è fondamentale che le informazioni riportate siano corrette ed affidabili.

2.5 ITGC

La base della struttura di controllo IT è definita dagli ITGC. Questi sono controlli interessati all'ambiente generale su cui sono sviluppati i sistemi IT.

Tra le tipologie di controlli gli ITGC stabiliscono un quadro generale di verifica per le attività IT, e sono definiti dalle policies e procedure utilizzate per supportare il corretto funzionamento delle applicazioni, dei controlli automatici implementati e dell'integrità dei report generati.

Attraverso i controlli ITGC è possibile effettuare una prima valutazione del livello minimo di sicurezza che deve essere garantito nella gestione di un sistema informatico, così che si possano assicurare le caratteristiche di:

- riservatezza delle informazioni e dei dati elaborati, accuratamente protetti dalla divulgazione non intenzionale;
- accuratezza delle transazioni, dei dati elaborati e delle informazioni che ne risultano;
- completezza delle informazioni che sono il risultato del processamento dei dati.

I controlli ITGC agiscono su due livelli dei sistemi informativi, un Layer Applicativo, relativo alla gestione del Sistema Informativo da analizzare ed un Layer

Infrastrutturale, volto ai supporti di ogni Applicativo, cioè il Sistema Operativo (SO) e il Database (DB).

Principalmente gli ITGC agiscono su 3 aree di controllo:

- **Manage Change**: controlli sulle modifiche, manutenzioni e aggiornamenti apportati agli applicativi IT e ad altri componenti rilevanti dell'ambiente IT.
- **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 se le informazioni trattate siano mantenute integre e che le loro elaborazioni siano state eseguite correttamente.

Vediamo ora come queste 3 aree sono trattate nello specifico, partendo dal processo di Manage Change. Questo racchiude nel suo interno le seguenti tipologie di cambiamenti:

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

A seconda delle modifiche effettuate viene attribuita una certa priorità ed un livello di rischio differente, così da definire diverse procedure di analisi.
In termini di impatto, i principali rischi che si possono incontrare in un processo di Manage Change sono definiti dai seguenti casi:

- gli 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.

Per quanto riguarda i controlli di Manage Access, questi mirano a verificare che nell'organizzazione in esame siano ben definiti i ruoli degli utenti e che siano rispettate le responsabilità associate alle varie utenze.
I Manage Access sono quindi suddivisi in controlli di:

- Password policy volti a individuare le parametrizzazioni di sicurezza adottate per confrontarle con quelle definite dalla società che effettua l'audit per verificare l'adeguamento agli standard;
- Utenze aventi ampi privilegi per verificare che questi siano un numero limitato e che rispecchino al personale autorizzato in base alle mansioni aziendali svolte;
- Processo di creazione/modifica utenze al fine di controllare che lo stesso segua il corretto iter di autorizzazioni;
- Processo di terminazione delle utenze per verificare l'effettiva terminazione delle utenze associate al personale dimesso.
- Analisi di SoD, ovvero la verifica della corretta segregazione delle funzioni, in particolare analizzando se nei processi di creazione o modifica utenze, le fasi di richiesta, approvazione e creazione siano gestite da persone diverse, con le corrette autorizzazioni.

Infine, i processi di Manage IT Operations volti a verificare che l'azienda in esame abbia un ambiente di elaborazione dei dati affidabile. Per effettuare questa analisi si verifica che le applicazioni adibite all'ottenimento dei backup delle informazioni funzionino in maniera corretta, e che i sistemi di immagazzinamento di questi dati non siano soggetti ad attacchi informatici. Nello specifico si controlla che:

- I backup vengono eseguiti periodicamente tramite appositi software e monitorati dal personale IT per verificare il completamento e la risoluzione corretta di eventuali errori;
- 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.

2.6 La procedura dei controlli ITGC

La procedura di un controllo ITGC è articolata in due fasi distinte che si succedono nel corso del periodo di analisi: la prima, quella definita dal WTT (Walk-Through Test), è necessaria ad ottenere il quadro di comprensione di come i controlli vengono effettuati, mentre la seconda è la fase effettiva di test, detto ToE (Test of Effectiveness), in cui si verifica l'efficacia stessa del controllo.
Vediamo adesso nello specifico come vengono affrontate le singole fasi durante il processo di audit.

2.6.1 Walk-Thorugh Test (WTT)

Durante la fase di walk-through si effettua l'analisi che viene definita come "design of control" con la quale si valuta se il controllo è stato disegnato in maniera efficace e, nel caso in cui dovessero venire intercettate delle mancanze o la struttura non risultasse adeguata alla copertura dei rischi relativi, verrebbe rilevata una deficiency nel disegno.
Attraverso quest'analisi si comprende quali sono le persone coinvolte 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 nella verifica che il controllo sia stato strutturato in maniera efficace per mitigare i rischi per cui è predisposto. Una volta 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.

2.6.2 Test of Effectivenesse (ToE) e Update Test (Roll Forward)

Successivamente alla fase iniziale di "walk-through" si effettua quella relativa alla valutazione dell'operatività stessa del controllo, ovvero la Test of Effectiveness (ToE). Durante questa fase, attraverso un'analisi effettuata su un

campione di item selezionati in maniera casuale, si verifica che il controllo funzioni come dichiarato e riscontrato nel disegno prestabilito; si controlla quindi che siano effettivamente seguiti tutti i passi prescritti nel disegno per capire se il risultato del controllo può essere definito "effective" o "ineffective".

Al fine di testare l'efficacia del controllo viene richiesto all'azienda revisionata di fornire un dettaglio di tutta la popolazione di item, relativi al periodo di campionamento in analisi.

Seguendo un approccio metodologico basato su un approccio risk-based, si effettua quindi un campionamento in base alla dimensione totale della popolazione, ovvero si estraggono, tramite appositi software di generazione casuale, un numero di item sui quali viene chiesto alla società di fornire evidenze dei controlli che sono stati effettuati.

Tramite l'analisi di queste evidenze il revisore IT può effettuare una verifica di ciò che è stato eseguito nei vari passaggi, accertandosi che gli attributi caratterizzanti sono stati rispettati.

Durante questa fase quindi risulta fondamentale il grado di accuratezza con cui vengono effettuati i campioni su cui si basa il controllo. Il campionamento infatti permette di fare delle valutazioni con un alto livello di confidenza, facendo sì che non sia necessario dover adottare un'analisi totale su tutti gli item della popolazione.

L'utilizzo di un campione porta tuttavia con sé un rischio, ovvero che l'efficacia venga del campione possa essere diversa da quella dell'intera popolazione. Per tale ragione vengono adottate metodologie di audit volte a effettuare dei campionamenti con un elevato intervallo di confidenza in modo da ridurre al minimo questo rischio.

Al termine della fase di testing viene quindi valutata l'efficacia del controllo, ovvero se il funzionamento di quanto descritto nel disegno dello stesso è stato rispettato nell'analisi dei vari item campionati. Infatti, se durante la fase di test vengono notate eccezioni rispetto a quanto descritto nel disegno, sarà compito dell'auditor stesso di indagare con la società per risalire alle cause di tali deviazioni.

Per concludere la fase ToE deve essere redatto un documento finale nel quale il revisore dovrà dettagliare i seguenti punti chiave:

- Il periodo di tempo coperto dal test;
- Descrizione del controllo;
- La numerosità della popolazione e del campione;
- La frequenza del controllo;
- Eventuali eccezioni riscontrate durante il test e con una spiegazione che dimostri che queste deviazioni trovate non invalidino il controllo;
- Conclusioni sull'efficacia operativa relative al periodo revisionato.

Quest prima fase di testing prende in analisi solo un determinato periodo di tempo dell'anno fiscale. Una volta terminato la fase di ToE, al fine di avere una piena copertura, vi è quindi una terza fase, quella di Update test: questa serve a verificare che nulla sia cambiato nelle procedure seguite dall'azienda nel periodo che intercorre dalla data di test alla fine dell'anno.
I test effettuati in questa terza ed ultima fase, possono essere svolti valutando diverse metodologie a seconda del periodo di tempo che si deve coprire: più il periodo è lungo e più sarà necessario effettuare dei test aggiuntivi, differentemente in caso di brevi intervalli di tempo, è necessario ricevere una conferma dalla società che i processi ed i controlli analizzati non abbiano subito modifiche successivamente alle valutazioni di test precedentemente eseguite.
Durante questa fase è necessario analizzare se vengono riscontrati problemi sul controllo il che significherebbe che uno o più rischi legati al processo dell'applicativo rimarrebbero scoperti andando a generare una deficiency.
Tutte le carenze che si incontrano nei controlli ITGC sono un ostacolo per il management nell'ottenere determinate informazioni finanziarie, il che ricade quindi sul corretto funzionamento dei controlli interni dell'azienda, con impatto sulle decisioni interne.[48]
Le deficiency possono quindi essere strutturali nel design, individuate mediante la fase di WTT, quando il controllo non è progettato in modo consono al funzionamento previsto; in alternativa le deficiency di tipo operativo sono identificate in fase di test, quando un controllo adeguatamente progettato non

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

funziona come previsto, o la persona che esegue il controllo non possiede l'autorità o competenza necessaria per eseguire il controllo in modo efficace.[49]
Nel momento in cui vengono identificate eccezioni al controllo è necessario quindi andare a stabilire se questo possa essere considerato ineffective, andando ad effettuare ulteriori analisi su come queste mancanze incidano in termini di rischi relativi. Si va valuta quindi la natura e le cause dell'eccezione, si determina l'eventuale sistematicità o casualità della stessa e si analizza quali siano gli effetti della deficiency sulle procedure di audit identificate.
Una volta stabilito ciò, si vede se l'eccezione ricada su un singolo attributo del controllo, perché in caso di test con più attributi, si verifica se tale insufficienza causa l'inefficacia dell'intero controllo. Nel caso in cui questa deficiency non influisca sull'efficace copertura dei rischi del controllo, quest'ultimo può essere valutato come effective.
In seguito alla presenza di deficency è possibile effettuare il test di sostanza sul controllo, ovvero, invece che testare solamente un campione della popolazione, si effettua un'analisi dell'intero processo in scopo, così da verificare effettivamente se l'eccezione trovata è sistematica oppure un caso isolato.

2.7 I controlli ITAC e ITDM

Ai fini di ottenere una accurata e completa analisi dei singoli processi di business della società revisionata, vengono designati ulteriori controlli sugli applicativi che permettono di prevenire o rilevare delle transazioni non autorizzate e di supportare il processo di auditing del bilancio.

In base alla natura del controllo, come visibile nella ***Figura 4***, possiamo definire due categorie:

- ITAC (IT Application Control), ovvero controlli automatici eseguiti sui sistemi applicativi della società che non richiedo un intervento manuale;

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

- ITDM (IT Dependent Manual), dei controlli che possono essere definiti ibridi, in quanto sono distinti sia da una componente manuale che una automatica.

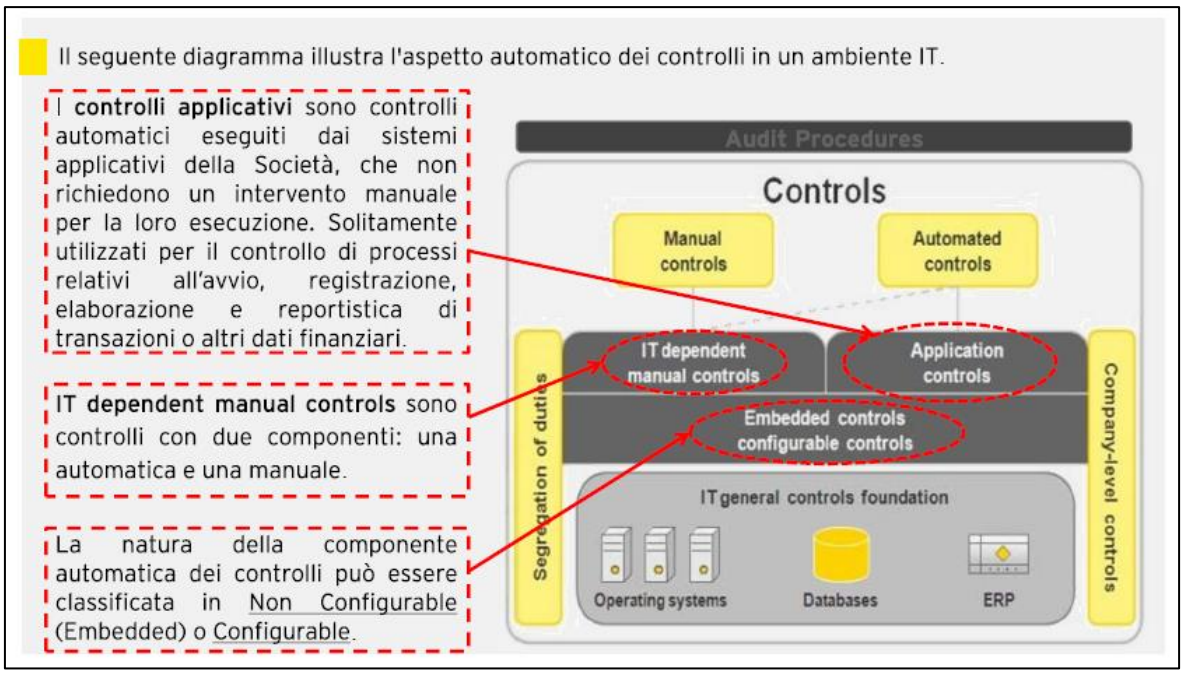


Figura 4 - Application Controls e ITDM - Definizioni

Per quanto riguarda gli ITAC, questi sono incorporati nei sistemi applicativi in quanto sono definiti da qualunque automatismo identificato nel sistema; possono includere impostazioni configurabili, algoritmi automatici, calcoli automatici e l'estrazione automatica di dati. Il test che viene effettuato serve a determinare se sono progettati, implementati e funzionanti in modo efficace.

Alcuni esempi di ITAC sono identificati in:

- Account payable (three-way match, approvazione da parte delle persone competenti degli ordini d'acquisto);
- Fixed assets (ad esempio le regole di ammortamento che calcolano in automatico le spese di ammortamento);
- Sales/ Account receivable (blocco degli ordini dei clienti se superano il loro limite di credito, emissione automatica della fattura una volta completata la consegna).

I controlli ITDM sono invece definiti come controlli a cui è associata sia una componente automatica che una manuale e sono caratterizzati dalla presenza di report generati dal sistema, detti IPE, che permettono di fornire dati utili alla revisione del management. Un esempio di ITDM può essere identificato nel processo di business della valutazione dei crediti verso clienti in cui, per valutare l'appropriatezza delle scadenze mensili, il revisore verifica manualmente la lista delle scadenze che è prodotta come report dalla contabilità dei clienti seguendo un processo automatico.

2.7.1 Test dei Controlli Applicativi

Il test sul funzionamento dei controlli automatici si effettua testando tutti i possibili scenari per ottenere evidenze sull'operatività degli stessi; gli scenari sono tutte le possibili casistiche che devono essere verificate e che possono essere designate in base alla natura del controllo.
Al fine di testare tutti gli eventi possibili si effettua un test di un "positive case", che verifica il normale e corretto comportamento del sistema a seguito dell'input atteso, ed un "negative case", volto a verificare l'efficacia risposta dell'applicativo nel caso in cui vengano inseriti dati in input non validi o di un eventuale comportamento imprevisto da parte dell'utente.
Se il test di entrambi gli scenari si conclude positivamente, il controllo può essere considerato effective.
Inoltre, nell'attività di test dei controlli applicativi si devono verificare quelle situazioni di rischio per le quali è possibile effettuare un override del controllo stesso; ovvero le situazioni in cui è possibile che il corretto funzionamento dell'applicativo sia alterato in modo da comprometterne l'efficacia. Un esempio sono le possibili modifiche alle soglie di tolleranza, per le quali va indagato chi può cambiare tali limiti per prevenire possibili azioni che rendano inefficace il controllo.

2.8 IPE, Information Produced by the Entity

Una IPE, Information Produced by the Entity, è una qualunque informazione prodotta da un sistema che può essere sia utilizzata per un controllo da parte della Società, sia dall'auditor per poter eseguire un'attività di controllo rilevante.

Le IPE sono quindi generate dalla Società nel momento in cui si fa uso di applicativi IT, tramite l'elaborazione l'utilizzo di tools di end user computing (EUC, elaborazione da parte degli utenti tramite Excel o PowerPoint) o in altre maniere (come alcune informazioni che vengono preparate manualmente).

Di base possono essere di varia tipologia a seconda del tipo di informazione che contengono, finanziaria, gerarchica o organizzativa, e si distinguono in base alla natura di chi l'ha prodotta, ovvero sia essa generata da un sistema informativo interno alla Società, o nel caso di un'entità con fornitori esterni, dalla società che ne eroga i servizi informativi.

Per effettuare il test delle IPE vengono valutati i seguenti rischi associati, schematizzati nella ***Figura 5***:

1. I dati elaborati dall'applicazione IT da cui viene prodotta 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.

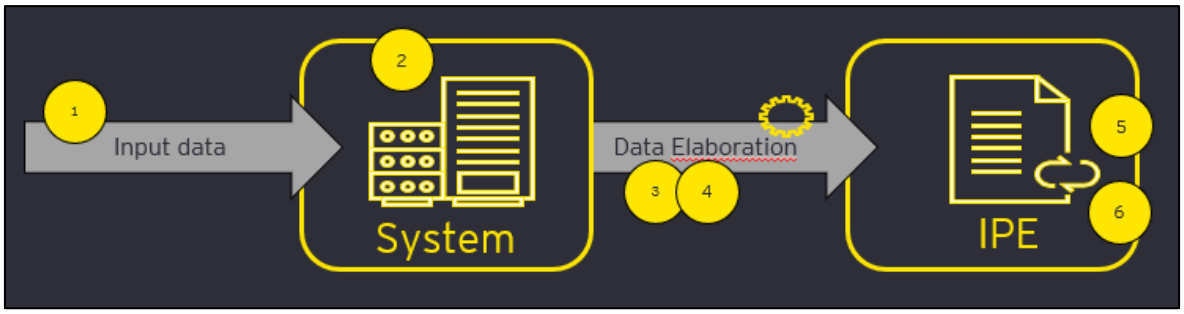


Figura 5 - Schema dei rischi delle IPE

All'interno dell'attività di supporto auditing IT vengono testati in particolare i rischi che fanno riferimento alla categoria di "IPE definition program", ovvero relative al programma di definizione 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 (relativi ai rischi 2 e 4).

Quando le IPE sono utilizzate per effettuare delle valutazioni nelle procedure di audit, è quindi necessario che anche queste siano testate al fine di verificare la completezza e correttezza delle informazioni. 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). Inoltre, quando le IPE sono generate da sistemi IT non verificati da ITGC o sono generate da programmi "Not Support", occorre allora validare anche il dato sottostante ed eventualmente considerare un test di sostanza o un direct testing laddove questo possa essere applicato.

2.9 Valutazione dei controlli e dei processi sottostanti

Al termine delle varie attività di testing degli applicativi, segue una fase di valutazione dei risultati ottenuti dove si determina se i controlli effettuati abbiano prodotto delle ragionevoli garanzie a copertura dei loro rischi associati.
Quando viene utilizzato una strategia ITGC-reliance, i controlli vengono valutati sulla base dei risultati dei test sostenuti, mentre in caso di strategia IT-substantive si considerano i risultati delle procedure di sostanza.
Vengono quindi determinate le seguenti valutazioni relative ai controlli e ai rischi:

- ITGC operating evaluation: è effettuata una valutazione operativa per ciascun ITGC (effective o ineffective) e, nel caso in cui un ITGC venga valutato come ineffective, è possibile che i rischi correlati ad esso vengano mitigati anche da altri controlli compensativi;

- IT process evaluation: si definisce, usando le valutazioni degli ITGC e/o qualsiasi procedura sostanza eseguita, se ogni processo IT rilevante affronti adeguatamente i rischi. Queste valutazioni sono usate per determinare le valutazioni IT aggregate per i controlli dell'applicativo e dell'ITDM. Le finali valutazioni finali possibili per l'IT proccess evaluation sono le seguenti:
    - Effective: il controllo per il processo IT ha funzionato efficacemente durante il periodo di audit.
    - Reliable: in caso di ITGC inefficaci, o sulla base dell'utilizzo di una strategia IT-substantive, sono utilizzate delle procedure di sostanza per verificare i rischi derivanti dall'uso dell'applicativo;
    - Ineffective: sono stati rilevati controlli non sufficienti e i test di sostanza, se effettuati, non possono fornire prove necessarie a stabilire che 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.
  Si valuta allora come:
    - "Support" quando i processi IT sono stati valutati come "effective" o almeno un processo è valutato "reliable" e i restati sono "effective"

- Not Support: i processi IT sono stati valutati come ineffective, ovvero se il funzionamento completo e accurato degli ITAC e degli ITDM non è supportato dal processo o dai processi IT correlati.

2.10 La relazione di revisione

La conclusione del ciclo di audit IT termina con la redazione di un documento finale in cui vengono comunicati al team di revisione contabile tutti i risultati ottenuti dei controlli testati al fine di accertare la veridicità dei dati contenuti nel bilancio.
Nel caso di revisione effettuata ai fini di ICFR il team di revisione deve quindi fornire un'opinione sull'efficacia del controllo interno della rendicontazione finanziaria, valutando le prove documentali, i possibili errori rilevati e qualsiasi carenza identificata sui controlli.
Il documento finale che accerta il giudizio in merito al bilancio della società revisionata viene redatto sotto forma di lettera la quale si articola in 3 paragrafi:

- Nel primo sono definite le responsabilità sulla redazione del Bilancio di Sostenibilità in carico all'azienda di revisione nei confronti degli amministratori della società cliente;
- Il secondo racchiude i principi di revisione di riferimento e vengono illustrate sommariamente le procedure adottate;
- Infine, l'ultimo paragrafo contiene il giudizio del revisore riguardo la conformità del bilancio societario rispetto ai principi contabili di riferimento, accertando dell'effettiva veridicità e correttezza della rappresentazione sulla situazione patrimoniale e finanziaria della società.

Questo documento di opinion viene quindi firmato dal partner della società di revisione che così facendo sancisce la conclusione del ciclo di audit.

Capitolo 3

3.1 Obiettivi del tirocinio

In questo capitolo sarà descritto il progetto di tirocinio curriculare che ho svolto presso la società EY, con l'obiettivo di inserimento nella realtà di questa azienda di consulenza, in particolare nella posizione di auditor IT a supporto della revisione contabile.

L'inserimento nell'azienda ha previsto una prima fase di formazione nella quale mi è stato presentato in primis il mondo dell'audit IT e di quali fossero i compiti di del team di audit IT all'interno di un processo di revisione contabile. Per introdurmi nelle tematiche oggetto delle attività del team di lavoro, mi è stato quindi illustrato il piano di auditing, attraverso un quadro complessivo delle attività che sono svolte lungo un intero ciclo ovvero: dalla fase di acquisizione del cliente, che è responsabilità dei partner e avviene partecipando alle gare di appalto, fino alla fase conclusiva di opinion sul bilancio che avviene tramite la stesura di una lettera di relazione di revisione del bilancio e dei sistemi informativi. Durante questa fase di introduzione sono stato affiancato nel mio percorso formativo da una figura Senior, la quale mi ha illustrato in maniera esaustiva le pratiche di auditing che avrei dovuto seguire da lì a breve; mi è stata spiegata la panoramica degli strumenti specifici di auditor utilizzati dalla società per effettuare le varie attività nel processo di revisione, dei tool aziendali e delle piattaforme online di comunicazione come il Canvas EY[50].

Date le tempistiche del mio inserimento nella società, arrivato in fase di chiusura del ciclo di audit, è stato importante, ai fini di svolgere delle analisi corrette e accurate, aver avuto un quadro completo dell'processo che il team di IT audit aveva svolto sul cliente fino alla definizione dello status di quell'istante temporale; la tracciabilità delle informazioni, raccolte attraverso una continua analisi di monitoraggio, è stato un'utile strumento di guida durante il mio ingresso. Inoltre, per poter aver una corretta nozione della metodologia di revisione e risk

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

management sviluppata internamente in EY, ho avuto modo di poter apprendere i concetti di base sulla gestione dei rischi informativi che traggono spunto dai principi standard forniti dalla SEC e PCAOB riguardo la sicurezza IT.

3.2 Il contesto aziendale

Nell'introdurmi all'interno di EY mi è stato insegnato qual sia il valore che la società assegna al cliente e con esso quali siano le modalità cui bisogna interloquire nell'approcciarsi durante il ciclo di audit. Il ruolo che ho ricoperto è stato quello di consulente informatico all'interno del ramo del "Technology risk"; il mio obiettivo è stato quello di occuparmi, supportando il team di revisione legale, delle attività relative ai controlli sulla gestione del rischio in ambito IT e assicurare all'azienda cliente il corretto svolgimento delle prassi nel rispetto della governance e delle compliance IT.

Nello specifico, sono stato inserito all'interno del team di IT Audit il cui organigramma vede a capo un Senior Manager, supportato da due Manager che dirigono diverse risorse tra cui consulenti Senior, con maggiore esperienza, e membri dello Staff in corso di formazione, tra cui il sottoscritto. La suddivisone dell'intero gruppo su due team di lavoro paralleli è dovuta alla gestione del carico di diversi progetti clienti del portafogli aziendale.

A seguito del mio ingresso nell'azienda, in cui per le prime due settimane ho seguito un percorso di formazione per introdurmi nel contesto della revisione IT, mi sono state assegnate una serie di attività per supportare diversi progetti di audit in corso d'opera. La mia entrata in azienda è avvenuta in un periodo finale del ciclo di audit in cui, come descritto nel precedente capitolo nella fase di Update Test, è stato necessario fare delle attività di inquiry con i responsabili IT dell'azienda cliente al fine di verificare che il corretto funzionamento degli applicativi, definito nel design del controllo, non avesse riscontrato cambiamenti o deficiency nell'ultimo periodo di analisi del ciclo di audit non coperto dalla precedente fase di test del ToE. Nell'effettuare le mie attività, è stato necessarie raccogliere, sia tramite interviste effettuate in modalità esclusivamente remota

che con comunicazioni via mail, dei feedback e delle informazioni necessarie alla conclusione di tutti i test.

3.3 Sviluppo di un Progetto di Audit IT

All'interno di questo capitolo vengono descritti nello specifico le attività che hanno interessato il ciclo di auditing di una società cliente appartenente al settore dell'automotive, che ricade sotto i canoni decretati dalla normativa SOX. La stessa verrà di seguito riportata come "Società X".
Le informazioni riportate faranno riferimento al progetto di audit relativo all'anno fiscale del 2019. La scelta è stata fatta poiché, nel momento in cui è stato scritto questo lavoro di tesi, il progetto di audit dell'anno in corso (anno fiscale 2020) era in corso di completamento, quindi, in accordo con la direzione della società EY, si è preferito utilizzare un progetto terminato per la completezza delle informazioni.

3.3.1 Comprensione dei processi di gestione ITGC

Come anticipato nel secondo capitolo, la prima fase del processo di controllo associato ai controlli ITGC prevede un momento preliminare in cui, attraverso un incontro che è stato effettuato in via telematica con il referente della Società X, sono state definite tutte le caratteristiche degli applicativi IT che sono oggetto di analisi nei controlli di revisione. Risulta infatti fondamentale andare a capire come è strutturato l'ambiente IT in cui sono inseriti i singoli applicativi, quali siano i processi ad esso relativi ed i controlli con la descrizione delle attività che l'azienda mette in atto per andare a minimizzare i rischi ad essi associati.

Tutte queste informazioni sono state riportate all'interno di un documento aziendale, il quale racchiude l'elenco dei rischi IT evidenziati sugli applicativi, i relativi controlli associati in copertura di ciascun rischio, e per ogni controllo l'elenco degli attributi che vengono testati.

Di seguenti saranno riportati degli esempi di processi che sono stati oggetto di revisione.

Analizziamo inizialmente il processo di **Manage Access (MA)**, ovvero il processo che prevede: la creazione o modifica delle autorizzazioni di un'utenza su un determinato applicativo, quali siano le persone che secondo le direttive della policy possono farne richiesta, come vengono trattate le utenze che vengono dismesse nel corso dell'anno fiscale ed infine quali sono i parametri di accesso ed autenticazione dei singoli applicativi.

Riguardo il processo di MA la società X ha quindi definito una serie di controlli e degli attributi testati a copertura dei rischi individuati per il processo.

Il processo di creazione utenza che ci è stato descritto è il seguente: la richiesta deve essere effettuata tramite apposito strumento di ticketing nel 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.
Nella ***Tabella 2*** che segue sono descritti gli attributi e i rischi associati al controllo.

Tabella 2 - Processo di User Provisioning

Titolo del processo	Scopo del controllo	Identificazione dei rischi associati	Attributi verificati nel processo
User Provisioning	Assicurarsi che l'accesso degli utenti e i nuovi diritti di accesso siano autorizzati e stabiliti in modo appropriato sulla base delle esigenze IT/Business.	R_MA2: Gli utenti dell'ambiente IT (IT e Business) non sono autorizzati. R_MA3: L'accesso degli utenti dell'ambiente informatico (IT e Business) crea problemi di segregazione dei compiti.	A. EY ha ispezionato l'elenco del personale responsabile di autorizzare i diritti d'accesso nuovi o supplementari e ne ha valutato l'adeguatezza. B. EY ha controllato che i diritti d'accesso nuovi o supplementari siano autorizzati dal personale identificato nell'attributo A. C. EY ha controllato che i diritti d'accesso nuovi o supplementari siano implementati dopo l'autorizzazione. D. EY ha controllato che l'implementazione dei diritti d'accesso nuovi o supplementari sia coerente con la richiesta approvata. E. EY ha controllato che l'approvatore e il proprietario dell'utente di destinazione siano diversi.

Per quanto riguarda il processo di terminazione utenze, schematizzato nella ***Tabella 3***, questo è stato descritto da un controllo che 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.

Tabella 3 - Processo di User Termination

Titolo del processo	Scopo del controllo	Identificazione dei rischi associati	Attributi verificati nel processo
User Termination	Assicurarsi che le User-ID degli "utenti terminati" siano revocate tempestivamente.	R_MA4: Gli utenti dell'ambiente IT (IT e Business) non sono appropriati.	A. EY ha controllato che gli utenti che hanno lasciato l'azienda siano disabilitati in modo tempestivo.

Per concludere la definizione dei processi di manage access, è stato definito il controllo associato alle direttive sulle password policy e gli accessi all'applicativo, definito come Logical Access in ***Tabella 4***, per il quale sono stati indicati quali sono

i requisiti delle password di autenticazione per accedere all'applicativo (lunghezza minima e massima, presenza o meno di caratteri speciali, ogni quanto bisogna cambiare la password, ecc.).

Tabella 4 - Processo di Logical Access

Titolo del processo	Scopo del controllo	Identificazione dei rischi associati	Attributi verificati nel processo
Logical Access	Le impostazioni della password sono appropriate all'ambiente e al livello di rischio.	R_MA1: (Autenticazione): Gli utenti dell'ambiente IT (IT e Business) non sono gli utenti previsti a causa di impostazioni di autenticazione e sicurezza inadeguate.	A. EY ha ispezionato le impostazioni delle password configurate e ne ha valutato l'adeguatezza secondo le pratiche principali.

Dopo aver stabilito il processo di manage access, si è passati a valutare le dinamiche che intercorrono dietro lo sviluppo di modifiche implementate per i sistemi applicativi in analisi; ovvero le procedure e i controlli effettuati per portare una modifica sull'applicativo.

Il processo descritto per il **Manage Change (MC)**, visibile nella ***Tabella 5***, prevede la formulazione di una richiesta associata alla change 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 incaricata provvede quindi a sviluppare la modifica e, una volta terminata, attende i risultati dei test effettuati 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 la fase di UAT (User Acceptance Test) da 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.

Tabella 5 - Processo di Manage Change

Titolo del processo	Scopo del controllo	Identificazione dei rischi associati	Attributi verificati nel processo
Manage Change	Assicurarsi che i test di accettazione soddisfino l'approvazione degli stakeholder e tengano conto di tutti gli aspetti dei piani di implementazione e conversione.	R_MC1: I nuovi programmi applicativi o le modifiche ai programmi esistenti, compresi i rapporti e le interfacce, non funzionano come descritto o richiesto perché non sono adeguatamente testati da persone appropriate diverse dagli sviluppatori.	A. EY ha controllato che la modifica sia stata testata. B. EY ha controllato che la data del test sia precedente alla data di implementazione della produzione.
	Assicurarsi che le modifiche siano autorizzate dai proprietari del business, dai responsabili dei servizi e/o dagli stakeholder tecnici IT.	R_MC2: Nuove implementazioni o modifiche a programmi, funzioni, interfacce o rapporti non sono approvate per l'ambiente né da un Punto Focale Business né da un Punto Focale IT.	C. EY ha ispezionato la lista del personale responsabile di autorizzare il trasporto delle modifiche in produzione e ne ha valutato l'adeguatezza. D. EY ha controllato che il trasporto della modifica in produzione sia autorizzato dal personale identificato nell'attributo A. E. EY ha controllato che la data di approvazione sia precedente alla data di implementazione della produzione.

Sempre nell'ambito del processo di MC, viene effettuto un test per verificare che sia rispettata la corretta segregazione delle responsabilità (SoD), ovvero che le persone che sviluppano una modifica siano diverse da quelle che la trasportano in produzione; questo, come descritto nella ***Tabella 6***, 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. Nel caso in cui ci sia un utente che, per necessità interne, abbia abilitazioni ad 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.

Tabella 6 - Segregation of Duties (SoD)

Titolo del processo	Scopo del controllo	Identificazione dei rischi associati	Attributi verificati nel processo
Segregation of Duties (SoD)	Assicurarsi che venga eseguito un monitoraggio regolare su sviluppatori e trasportatori (segregazione a livello di diritti di accesso).	R_MC3: I programmi in produzione non sono protetti permettendo agli sviluppatori di spostare modifiche non autorizzate o non testate nell'ambiente di produzione.	A. EY ha ispezionato che i proprietari degli utenti con il permesso di sviluppare le modifiche nell'ambiente di sviluppo/certificazione sono appropriati. B. EY ha ispezionato che i proprietari degli utenti con il permesso di trasportare le modifiche nell'ambiente di produzione sono appropriati. C. EY ha ispezionato che la segregazione dei doveri tra l'attributo A e l'attributo B è osservata.

L'ultimo processo di manage change, individuato per uno specifico applicativo in scopo, riguarda il controllo effettuato sull'apertura del mandante, ovvero il client dell'ambiente di produzione, mostrato nella ***Tabella 7***. Il client è chiuso in produzione; in casi di estrema necessità, con un'autorizzazione specifica, il client può essere aperto tramite SUID ICT, ovvero una super utenza con accesso a particolari privilegi. Al fine di monitorare le modifiche svolte in produzione, l'apertura del client e le conseguenti azioni in produzione vengono automaticamente registrate se il settaggio l'impostazione parametrica è corretta. Per ogni apertura del mandante, la Società X deve accertarsi di inserire i parametri di corretta chiusura del client in modo che siano settati secondo la leading practice internazionali.

Tabella 7 - Client Opening monitoring

Titolo del processo	Scopo del controllo	Identificazione dei rischi associati	Attributi verificati nel processo
Client Opening monitoring	Assicurarsi che tutte le attività di apertura dei clienti siano adeguatamente tracciate e pre-approvate.	R_MC4: I programmi / personalizzazioni dell'ambiente di produzione non sono protetti permettendo così agli utenti di fare cambiamenti direttamente nell'ambiente di produzione.	A. EY ha controllato che i parametri CCCORACTIV, CCNOCLIIND, CCCOPYLOCK, REC/CLIENT siano impostati correttamente. B. EY ha ispezionato la lista del personale responsabile di autorizzare le attività di apertura del cliente e ne ha valutato l'adeguatezza. C. EY ha controllato che i SUID in grado di aprire il cliente siano assegnati al personale appropriato. D. EY ha controllato che le attività di apertura del cliente siano autorizzate dal personale identificato nell'attributo B. E. EY ha controllato che le attività di apertura del cliente siano autorizzate prima dell'implementazione. F. EY ha controllato che le attività di apertura del cliente siano eseguite solo dai SUID identificati nell'attributo C.

Un ulteriore controllo che il referente della Società X ha definito nella fase di Understanding è il controllo di Manage Operations (MO), ovvero un controllo che monitora con quali job automatici e sistemi di backup si garantisce l'integrità e l'archiviazione delle informazioni prodotte e la loro schedulazione.

Nello caso specifico, illustrato nella ***Tabella 8***, il referente ha chiarito che il controllo giornaliero dei job automatici viene effettuato per mezzo di una società esterna; quest'ultima esegue quotidianamente un monitoraggio dell'esito dei job. Se un job finisce in errore, il responsabile delle attività di job scheduling procede all'identificazione del problema e alla sua repentina risoluzione.

Tabella 8 - Processo di Job Monitoring

Titolo del processo	Scopo del controllo	Identificazione dei rischi associati	Attributi verificati nel processo
Job monitoring	Assicurarsi che i lavori critici nell'ambiente di produzione siano monitorati e che i risultati inaspettati siano affrontati in modo appropriato.	R_MO2: I problemi con i programmi che non possono essere portati a termine non sono affrontati o sono affrontati in modo inappropriato	A. EY ha controllato che il personale coinvolto nel monitoraggio del lavoro sia appropriato.

3.3.2 Test di Walk-Through

Proseguendo con la fase di Walk-Through, come già descritto nel secondo capitolo, è presente una fase di test definita Test of Design nella quale, tramite analisi che si effettuano mediante le evidenze raccolte dal referente della Società X, si valuta se i controlli sono stati disegnati in maniera efficace, ovvero se la procedura di controllo descritta dall'azienda sia valida a mitigare i rischi IT.

Per ogni processo definito precedentemente abbiamo quindi raccolto delle evidenze utili all'auditor per stabilire se il controllo sia indirizzato in maniera corretta verso la copertura dei rischi associati e che il funzionamento sia il medesimo di quanto già definito.
Di seguito sono riportati esempi dei Test di WT effettuati sui processi in audit.

User Provisioning - Creazione di una nuova utenza

Richiesta di creazione utenza (***Figura 6***) – In data 18/03/2019 attraverso il sistema di ticketing di SharePoint aziendale è stata richiesta da Chiara, responsabile della Business Unit di Internal Control, la creazione della nuova utenza di Anna. (Attributi B-C-D-E).

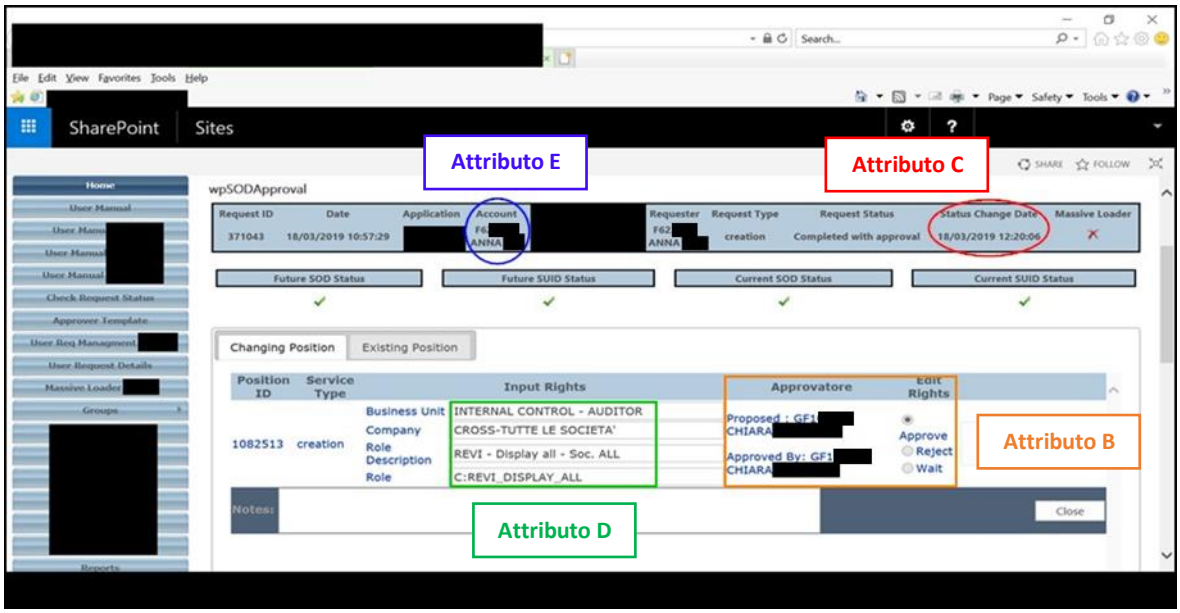


Figura 6 – Attributi B-C-D-E - Richiesta di creazione utenza

Approvazione alla creazione (Figura 7) – Nella schermata di SharePoint è possibile verificare che la richiesta di creazione è stata approvata (Attributo B).

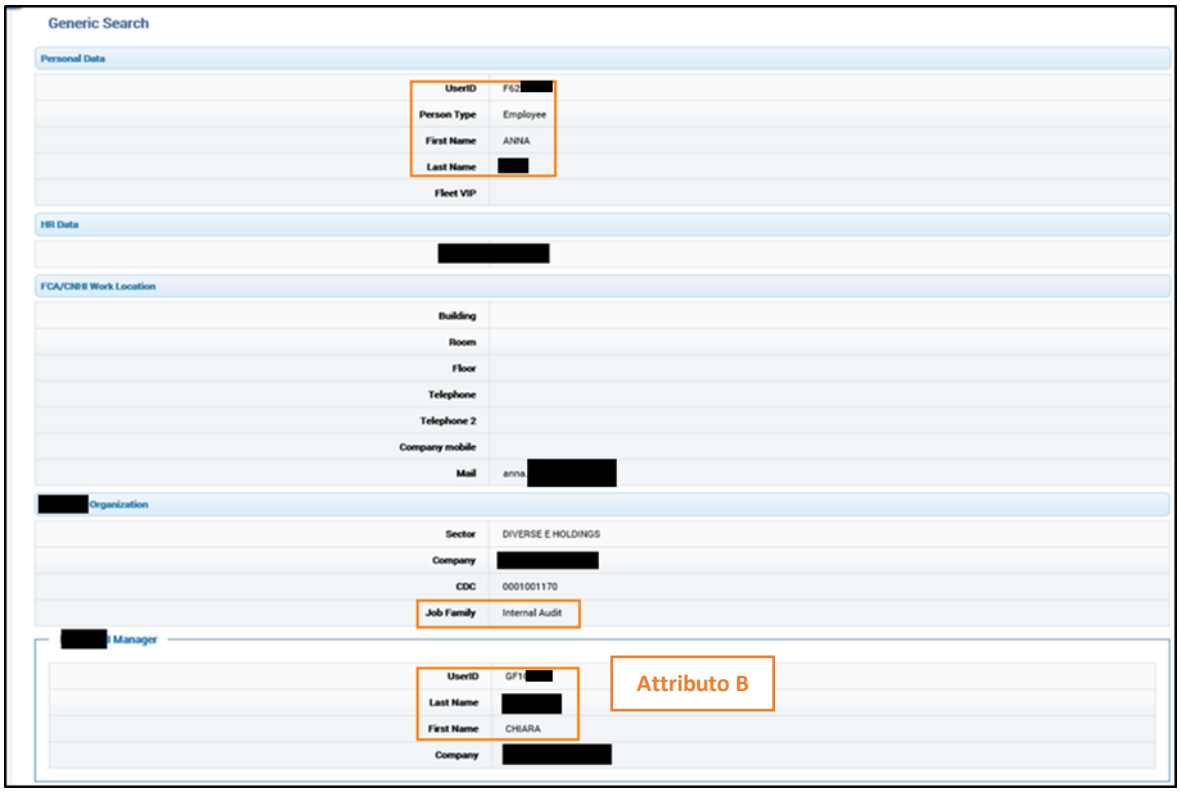


Figura 7 – Attributo B - Approvazione alla creazione dal tool SharePoint

Creazione dell'utenza (***Figure 8 - 9***) – Una volta approvata, in data 18/03/2019 l'utenza di Anna viene creata. Per sapere quali ruoli sono stati assegnati al nuovo utente, è necessario estrarre una tabella che contiene il riferimento ai ruoli richiesti (Attributo C-D).

Figura 8 - Estrazione da Database

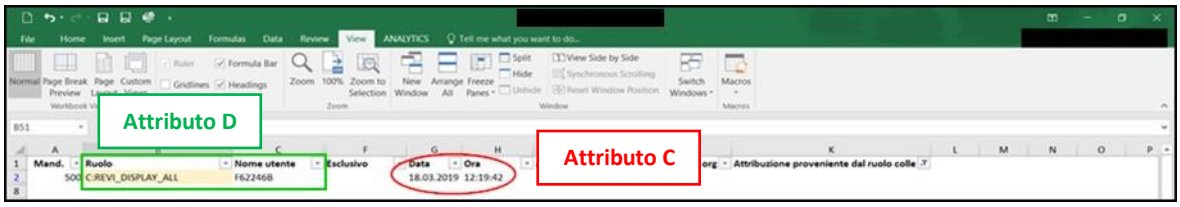


Figura 9 - Attributi C-D - Estrazione da tool dell'applicativo

User Termination

Nel processo di terminazione la società X effettua un controllo sull'utenza di Luca che, essendo una persona in uscita dall'azienda, sia correttamente disabilitata sull'applicativo in scopo. Di seguito riportata la schermata relativa alla terminazione utenza dell'applicativo in scopo. ***Figura 10***.

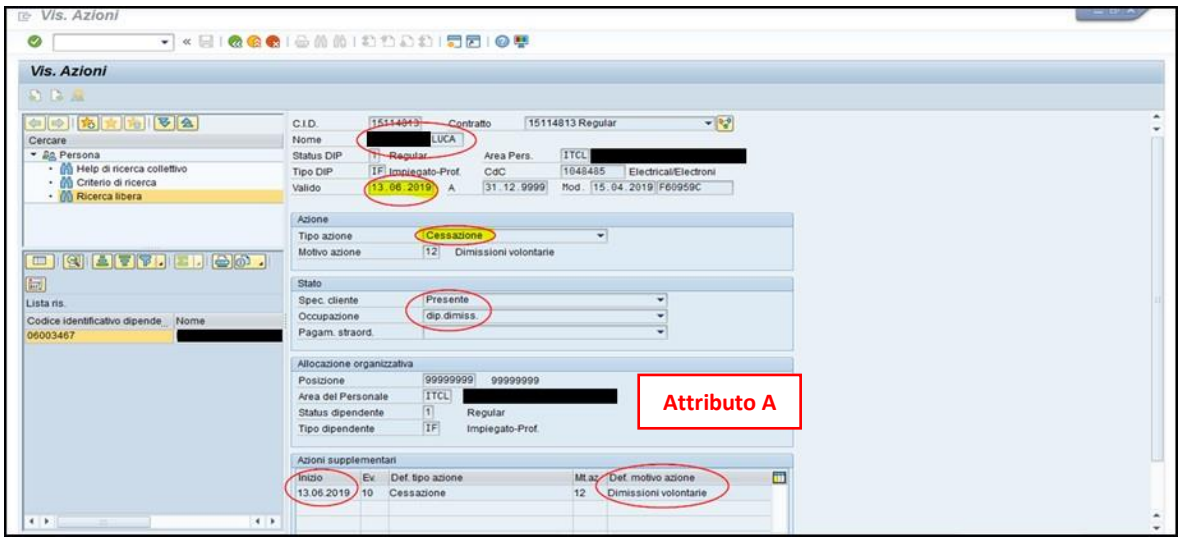


Figura 10 – Processo di terminazione utenza

Nella schermata di sotto (***Figura 11***) è possibile vedere come nell'applicativo gestionale della Società venga settato lo status di "inactive".

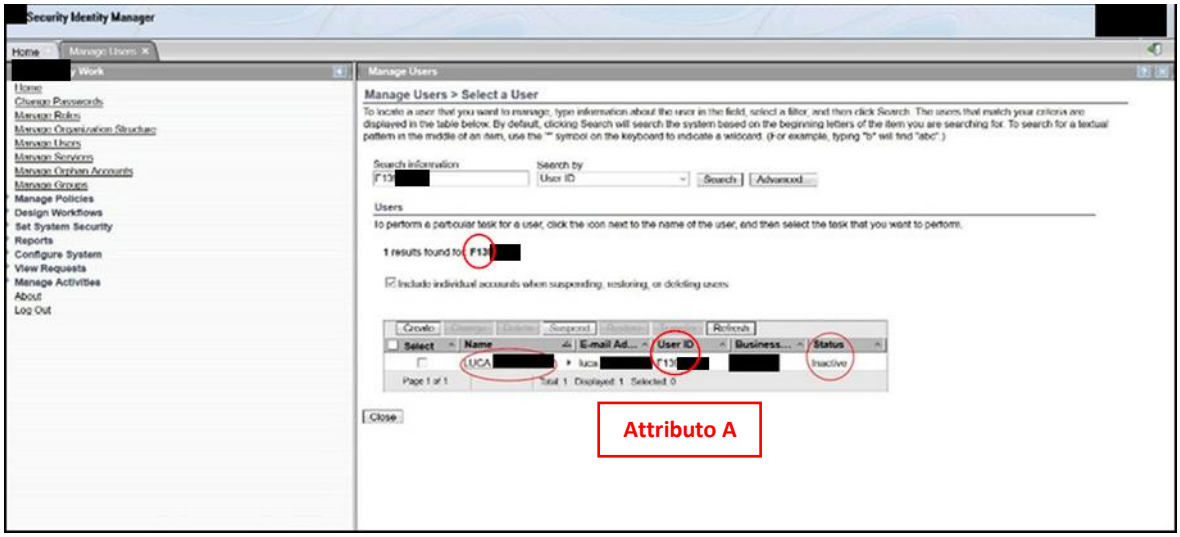


Figura 11 - Attributo A - Terminazione utenza sull'applicativo gestionale

Dalla schermata di visualizzazione dell'applicativo testato, visibile in ***Figura 12***, si evince che l'utenza F13ZZZ associata a Luca risulti terminata (Attributo A).

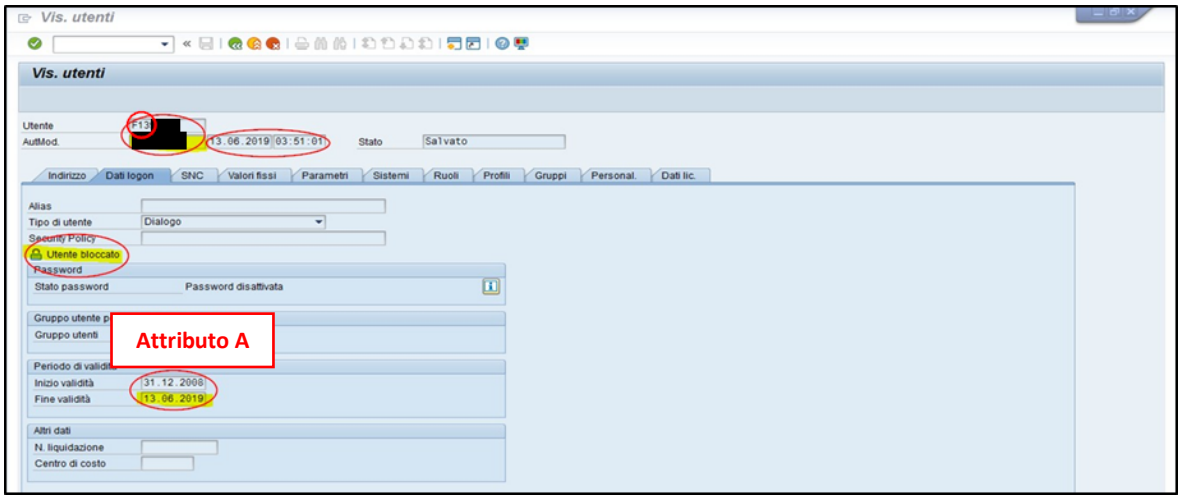


Figura 12 - Conferma terminazione utenza da applicativo

Manage Change

Sviluppo e Validazione UAT – In data 16/05/2019, come visibile dalla mail in ***Figura 13***, viene richiesta l'approvazione formale all'approvazione dei test effettuati per la CR relativa la Progetto in analisi. (Attributi A-B)

Figura 13 - Attributi A-B - Mail Validazione fase di UAT

Richiesta autorizzazione trasporto (***Figura 14***) – una volta completatala fase di test, in data 22/05/2019, Roberto della Società X richiede l'autorizzazione all'ICT manager Simonetta la quale dà l'ok a procedere con il passaggio in produzione della CR (Attributo C-D).

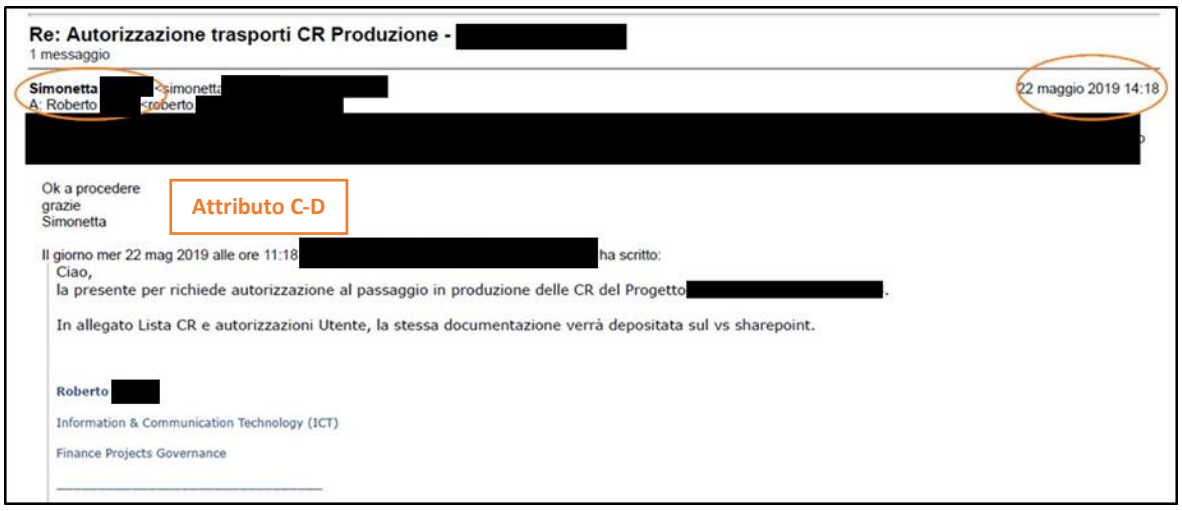


Figura 14 - Attributo C-D - Mail Richiesta autorizzazione al passaggio in produzione

Dopo aver ottenuto l'autorizzazione, la change viene trasportata in ambiente produzione come si evince dalla schermata sottostante ***Figura 15***. (Attributo E).

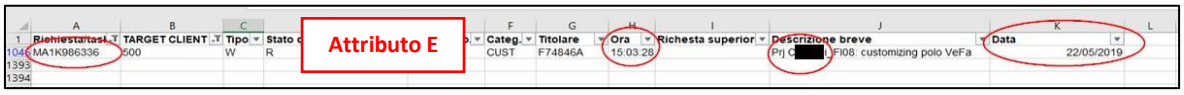


Figura 15 - Attributo E - Trasporto in produzione

Client Opening Monitoring

Nel controllo sul monitoraggio delle aperture del mandante si verifica che i parametri definiti per il Mandante YYY in esempio siano settati correttamente secondo le leading practice aziendali, che come visibile nella TabellaZ sono rispettivamente i valori 2-3-X (Attributo A, ***Figura 16***).

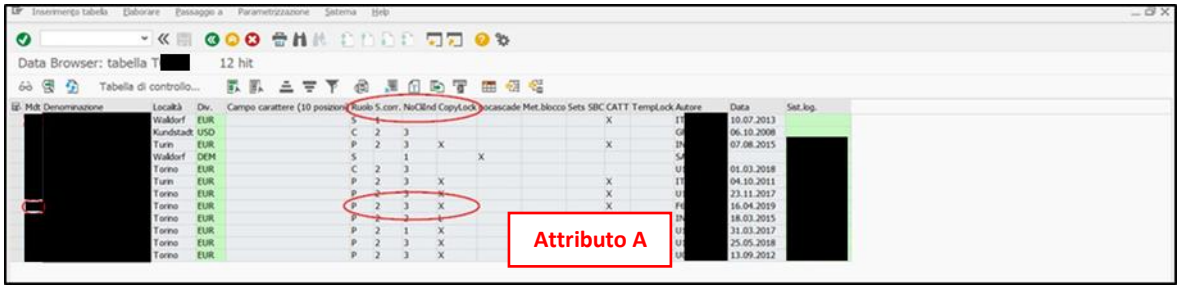


Figura 16 – Attributo A - Estrazione TabellaZ aperture Mandante

La società ha verificato che gli utenti che hanno effettuato le aperture del Mandante YYY siano delle SuperUtenze (SUID) con appropriati grant autorizzativi (Attribuiti C-F, ***Figura 17***).

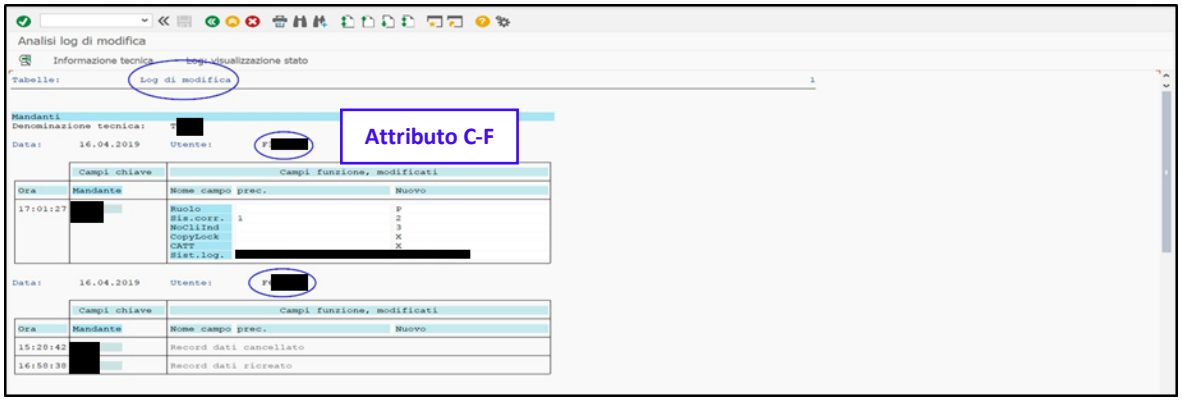


Figura 17 - Attributi C-F – Evidenza utenze SUID

Infine, è stato verificato che l'attività di apertura fosse stata autorizzata da un Responsabile dell'area di Business adeguato (Attributi B-D-E, ***Figura 18***).

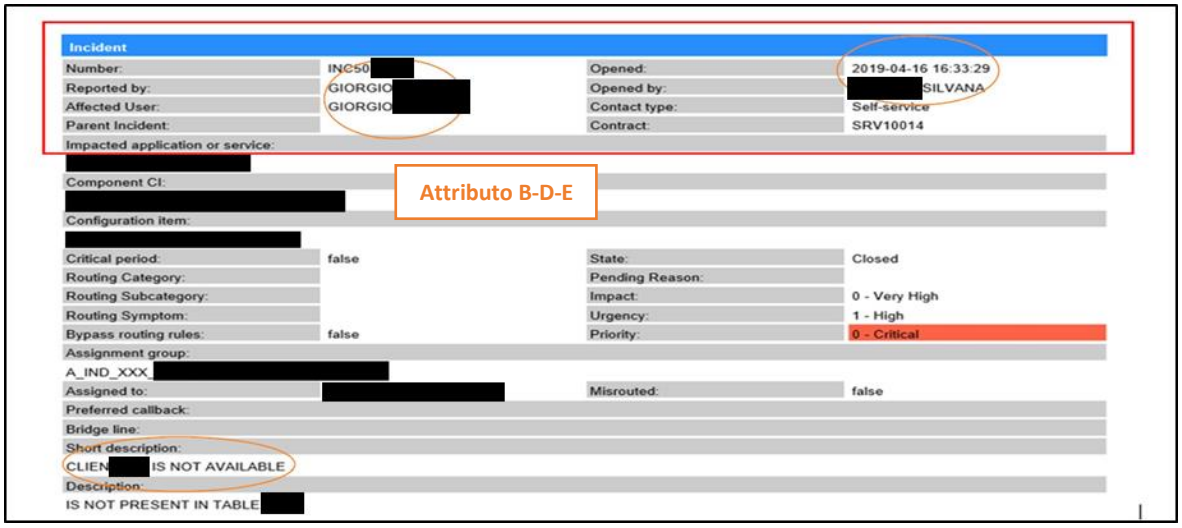


Figura 18 - Attributi B-D-E - Ticket di autorizzazione apertura mandante

Job Monitoring

Verifica della corretta esecuzione – Per il controllo dei job è necessario verificare che questi ultimi siano completati correttamente, come indicato in ***Figura 19***, di conseguenza è stato considerato un job in riferimento la settimana dal 27/08/2019 al 02/09/2019.

Figura 19 - Mail conferma completamento attività Job

Come si vede dall'immagine, l'utente Application Management System (AMS) della società fornitrice per l'azienda X, riporta l'esito correttamente avvenuto del Job

in campione. L'utenza di Marco risulta essere appropriata alla mansione richiesta (Attributo A, ***Figura 20***).

Entity	[redacted]		
Application	[redacted]		
Application description	HR process management		
Product/Package Name	Standard Package		
Instance	Single Instance		
Application owner	[redacted] Marco		
Service manager	Marco		
IT Control owner	Marco		
AMS provider	[redacted]	**ITO provider**	[redacted]

Attributo A

Figura 20 - Attributo A - Ticket application owner del Job

Dalla schermata sottostante è possibile verificare che tutti i job che hanno girato in data 27/08/2019 risultano conclusi con esito positivo (Attributo B, ***Figura 21***).

	A	B	C	D	E	F	G	H
1	Job Name	Start Dat	Start Tir	End Date	End Tir	Job Created I	Status	Duration(second
2	ALL_ROLES	27/08/2019	02:00:14	27/(				5.049
3	AMERICAS_BAUS02_000	27/08/2019	04:47:54	27/(				1.610
4	AMERICAS_BAUS02_001	27/08/2019	04:47:54	27/(				1.022
5	AMERICAS_BAUS02_002	27/08/2019	04:47:54	27/(				642
6	AMERICAS_BAUS02_003	27/08/2019	04:47:54	27/(				328
7	AMERICAS_BAUS02_004	27/08/2019	04:47:54	27/(				337
8	AMERICAS_BAUS02_005	27/08/2019	04:47:54	27/(				384
9	AMERICAS_BAUS02_006	27/08/2019	04:47:54	27/(				855
10	AMERICAS_BAUS02_007	27/08/2019	04:47:54	27/(				486
11	AMERICAS_BAUS02_008	27/08/2019	04:47:55	27/(				711
12	AMERICAS_BAUS02_009	27/08/2019	04:47:55	27/(				316
13	AMERICAS_BAUS02_010	27/08/2019	04:47:55	27/(				378
14	AMERICAS_BAUS02_011	27/08/2019	04:47:55	27/(				421
15	AMERICAS_BAUS02_012	27/08/2019	04:47:55	27/(				369
16	AMERICAS_BAUS02_013	27/08/2019	04:47:55	27/(				338
17	AMERICAS_BAUS02_014	27/08/2019	04:47:55	27/(				289
18	AMERICAS_BAUS02_015	27/08/2019	04:47:55	27/(				416
19	AMERICAS_BAUS02_016	27/08/2019	04:47:55	27/(				405
20	AMERICAS_BAUS02_017	27/08/2019	04:47:55	27/(				598
21	AMERICAS_BAUS02_018	27/08/2019	04:47:55	27/(				892
22	AMERICAS_BAUS02_019	27/08/2019	04:47:56	27/(				818
23	AMERICAS_BAUS02_020	27/08/2019	04:47:56	27/08/2019	04:48:01	BATCH_USER	Finished	5
24	BGENH001_GHR1000101	26/08/2019	20:00:33	26/08/2019	20:14:45	ITSSCHED03	Finished	852
25	BR_OM_EXPORT_FIRST	26/08/2019	15:00:01	26/08/2019	19:27:55	FGHACN020	Finished	16.074
26	C4T_APPROVER_&_POLICY_UPDATE	26/08/2019	23:40:04	27/08/2019	00:45:36	FGHACN141	Finished	3.932
27	CENTRAL_EUROPE_BAUS02_000	27/08/2019	02:47:24	27/08/2019	04:38:23	BATCH_USER	Finished	6.659

Figura 21 - Attributo B – Estrazione esiti attività dei Job

3.3.3 Test of Effectiveness (ToE)

Dopo aver verificato nella fase di WTT che i controlli siano stati disegnati in modo appropriato per valutare i rischi loro associati, si è passati alla fase successiva di ToE, con la quale si è verificata l'efficacia del test. Durante questa fase è stato quindi necessario formulare dei campioni di item per ciascun controllo osservato durante il Test of Design.

La formulazione dei campioni è necessaria per tutti quei controlli che sono caratterizzati da una definita popolazione di item che viene definita tramite un estrazioni o report forniti dal referente della Società X. Le popolazioni che definiamo per un determinato processo molto spesso sono rappresentate all'interno di estrazioni o report di applicativi come Excel o ACL, in cui sono indicate date e codici indentificativi per ogni singolo item.

Andiamo ora ad analizzare come esempio la popolazione campionata per il controllo di User Provisioning: per questo controllo è stato necessario richiedere alla Società X le estrazioni, per ciascun applicativo in scopo, di tutte le utenze e dopo di che, in base ai criteri definiti nel test of design, sono stati filtrati i campi di "Azione", con riferimento alle modifiche che riguardano esclusivamente la creazione (indicati in figura dalle voci "Utente creato"), e la tipologia di user che ai fini del test sono identificate da utenze di tipo dialogo, quelle che hanno accesso diretto al sistema e di tipo servizio (indicati in ***Figura 22*** dalle voci "A dialogo"). Oltre alla popolazione, secondo la prassi dettata dalla metodologia societaria, ci siamo fatti fornire evidenze di completezza, ovvero degli elementi che hanno lo scopo di provare che l'estrazione iniziale di item che ci è stata trasmessa non sia stata manomessa e che contenga effettivamente tutte le informazioni relative al periodo di audit. Nell'immagine sottostante è illustrato un esempio di schermata di completezza nella quale è possibile vedere il numero di record contenuti nella tabella e il giorno in cui tale importazione di dati è stata scaricata al fine di verificare che il report relativo alla popolazione iniziale corrisponda in termini numerici.

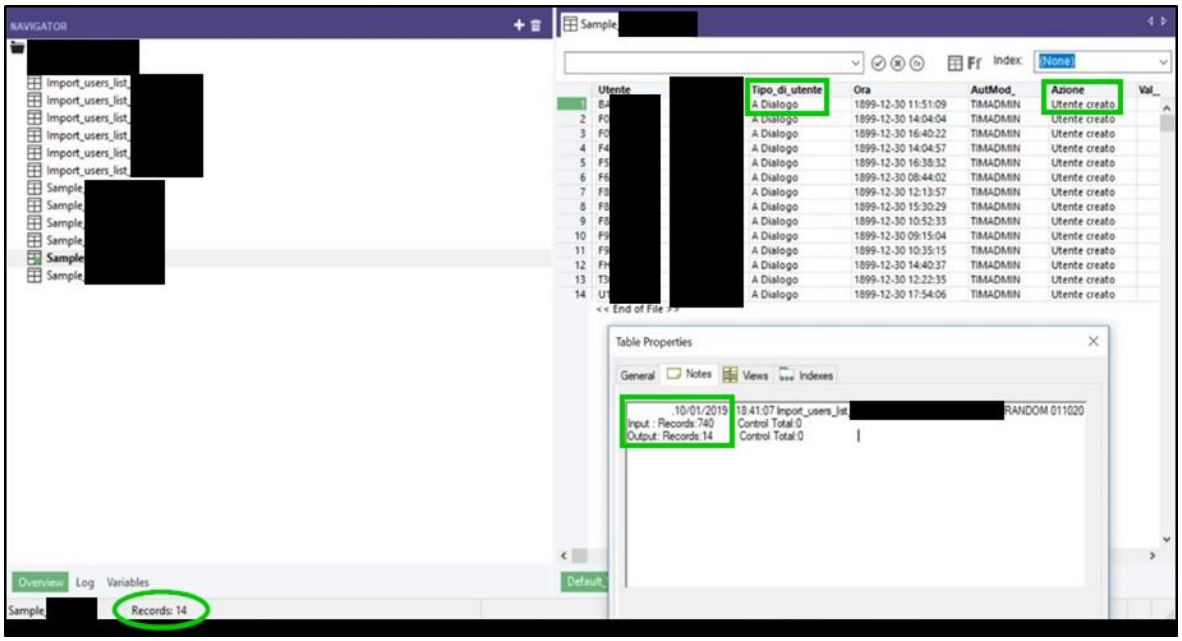


Figura 22 - Schermata di completezza dell'estrazione delle utenze

Per identificare il cluster di tutte utenze oggetto di analisi bisogna inoltre filtrare solo quelle con data di ultima modifica facente riferimento al periodo oggetto di audit, in tal caso compreso dal 01-01-2019 al 10-01-2019 per la fase di ToE.

Dopo aver eseguito questi passaggi e appurata la completezza delle informazioni, si ottiene quindi la popolazione totale su cui abbiamo potuto effettuare un campionamento casuale tramite l'utilizzo di un tool aziendale interno. È fondamentale infatti che gli item selezionati siano generati da una selezione randomica per poter trarre delle conclusioni affidabili sull'intera popolazione del campione. Secondo la metodologia adottata, la dimensione del campione corrisponde al 10% della popolazione totale, con un minimo di 5 unità (a meno che il totale sia inferiore, in tal caso verrà considerata l'intera popolazione) ad un massimo di 25 item.

Dopo aver determinato i campioni dei processi in analisi, questi sono stati mandati al referente della società X a cui è stato richiesto di raccogliere evidenze per tutti gli item selezionati; una volta ottenute le evidenze abbiamo quindi proceduto con la formalizzazione delle stesse.

Questa fase del processo di audit è solitamente la più lunga del ciclo perché richiede un dispendio oneroso di tempo sia per la raccolta delle evidenze da parte del referente, sia per formalizzare i documenti degli item, come spesso accade in

particolare quando i campioni sono costituiti da una numerosità elevata. La formalizzazione dei documenti avviene su form specifici che contengono le informazioni necessarie all'analisi. 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'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.

Nella ***Figura 23*** è mostrata la tabella riassuntiva che abbiamo costruito per la selezione del campione del test sulle utenze dell'applicativo in analisi.

Procedura di Test

		Attributi del processo								
		R_MA2				R_MA3				
Testing #	Item identificativo	Approvato da	A	D	Approvato nel	Creata nel	B	C	Creata da	E
1*	F613[redacted]	[redacted]	X	X	05.28.2019	05.28.2019	X	X		X
2*	F233[redacted]	[redacted]	X	X	01.21.2019	01.24.2019	X	X	[redacted]	X
5*	F586[redacted]	[redacted]	X	X	07.12.2019	07.12.2019	X	X		X
7*	F62246B - [redacted]	CHIARA [redacted]	X	X	03.18.2019	03.18.2019	X	X		X
14*	F819[redacted]	[redacted]	X	X	03.14.2019	03.14.2019	X	X		X
22*	F257[redacted]	[redacted]	X	X	06.13.2019	06.17.2019	X	X		X

Procedure eseguite [redacted]	
A	EY ha controllato che i diritti di accesso nuovi o aggiuntivi siano autorizzati dalla persona appropriata.
B	EY ha controllato che i diritti di accesso nuovi o aggiuntivi siano implementati dopo l'autorizzazione.
C	EY ha controllato che l'attuazione dei diritti d'accesso nuovi o supplementari sia coerente con la richiesta approvata.
D	EY ha ispezionato la lista del personale responsabile di autorizzare i diritti di accesso nuovi o aggiuntivi e ne ha valutato l'adeguatezza.
E	EY inspected that the implementer and the approver are different.

Note chiave:	
X	Attribute satisfied without exception.

Figura 23 - Tabella riassuntiva ToE

Dalla tabella è possibile risalire agli item relativi al campione di utenze create richiesto ai referenti della società X; sono indicati il codice utenza identificativo nella società, il responsabile che ne ha autorizzato la creazione con la rispettiva data di autorizzazione, l'utenza che ha effettuato la creazione e la data in cui è stata realizzata sull'applicativo.
Come si può notare, nella parte destra della tabella sono presenti tutti gli attributi dei controlli specificati nel riquadro in basso.

Infine, nella Figura 24 è mostrata la tabella conclusiva nel quale viene indicato l'esito del test sul controllo e la presenza o meno di eccezioni, che per il controllo

specifico non risultano presenti. Nel caso in cui si presentassero delle anomalie durante la fase di test devono essere riportate aggiungendo una casella indicando le eccezioni riscontrate, 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.

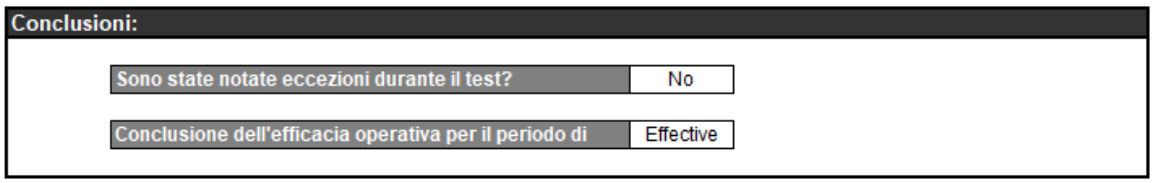


Figura 24 - Tabella di Conclusion del ToE

I documenti rappresentati nelle tabelle precedenti sono una riproduzione degli aspetti salienti di quelli utilizzati dall'azienda per la formalizzazione dei test sui controlli ITGC, poiché, per ragioni di segretezza aziendale non è permesso riportare il file originale. Inoltre, per le stesse ragioni anche il nome del software per effettuare il campionamento non è stato riportato.

3.3.4 Test degli ITAC

Come descritto nel secondo capitolo, la prima fase necessaria a testare i controlli sulle componenti automatiche è stata effettuata dal team di revisione IT che, a seguito di un colloquio con il cliente, ha individuato le SCOTs relative alle informazioni di bilancio, ed è stato determinato quali fossero gli applicativi sui quali dover concentrare le analisi.
I controlli ITAC sono controlli messi in atto sugli automatismi individuati negli applicativi dell'azienda cliente; si definiscono ogni qual volta si effettua un'operazione completamente automatizzata la quale deve essere verificata affinché funzioni correttamente.
I test degli ITAC sono svolti diversamente rispetto a quelli effettuati sugli ITGC poiché, trattandosi di automatismi del sistema, devono funzionare sempre allo stesso modo e quindi, in base a quanto definito tramite la fase di Understanding su come funziona l'automatismo, segue una fase di test of control nella quale sono

verificati gli scenari che si possono ipotizzare per appurare il corretto funzionamento del controllo.
Generalmente gli scenari sono definiti da un "negative test", per cui si verifica che le azioni non permesse non vengano effettivamente eseguite, ed un "positive test" dove ci si accerta che tutte le azioni possibili vengano correttamente realizzate.
Di seguito verrà descritta la formalizzazione di un ITAC che fa riferimento al processo di registrazioni delle fatture per un applicativo in revisione.

Registrazione fatture: Al fine di verificare il corretto funzionamento dell'automatismo dell'applicativo in scopo, la società X ha effettuato un "positive test" per verificare una corretta risposta del sistema all'utilizzo di opportuni input.
Dal menù "Coda di stampa", mostrato nella ***Figura 25***, è stato selezionato un articolo da fatturare, che viene indicato con la voce "TODPRT".

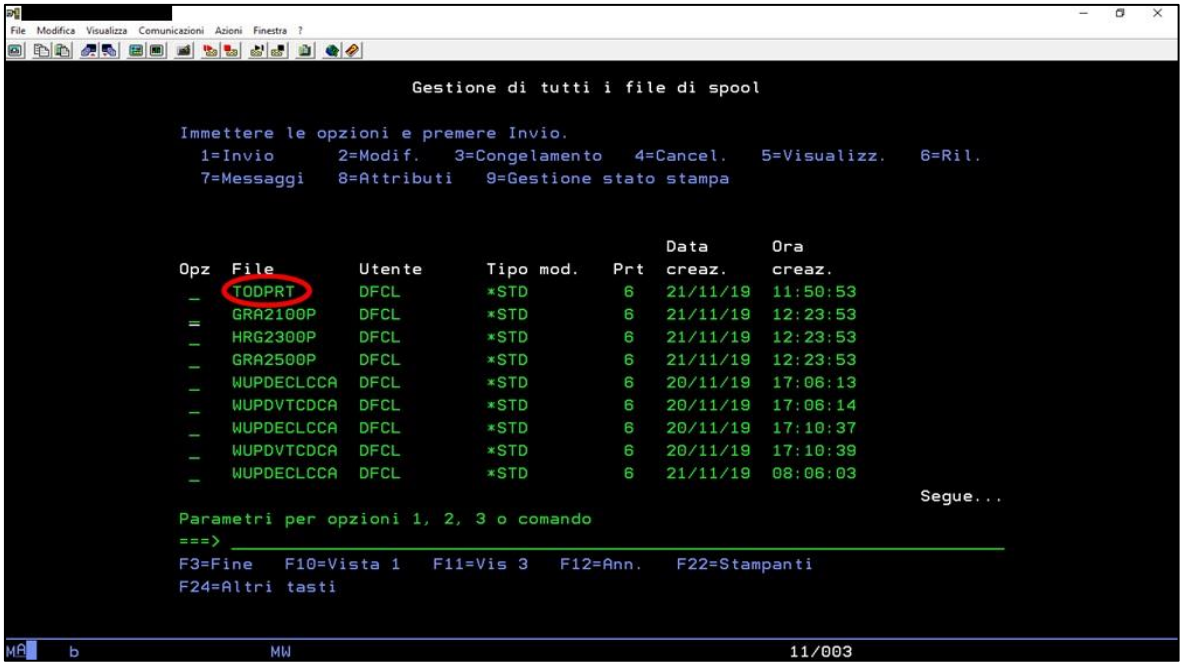


Figura 25 - Schermata di selezione articolo da fatturare

Il report "XXX" riportato nel file Excel sottostante, che è stato scaricato prima di effettuare il test, mostra l'ultima fattura disponibile (nella "Colonna I" della ***Figura 26***) con numero documento "48887".

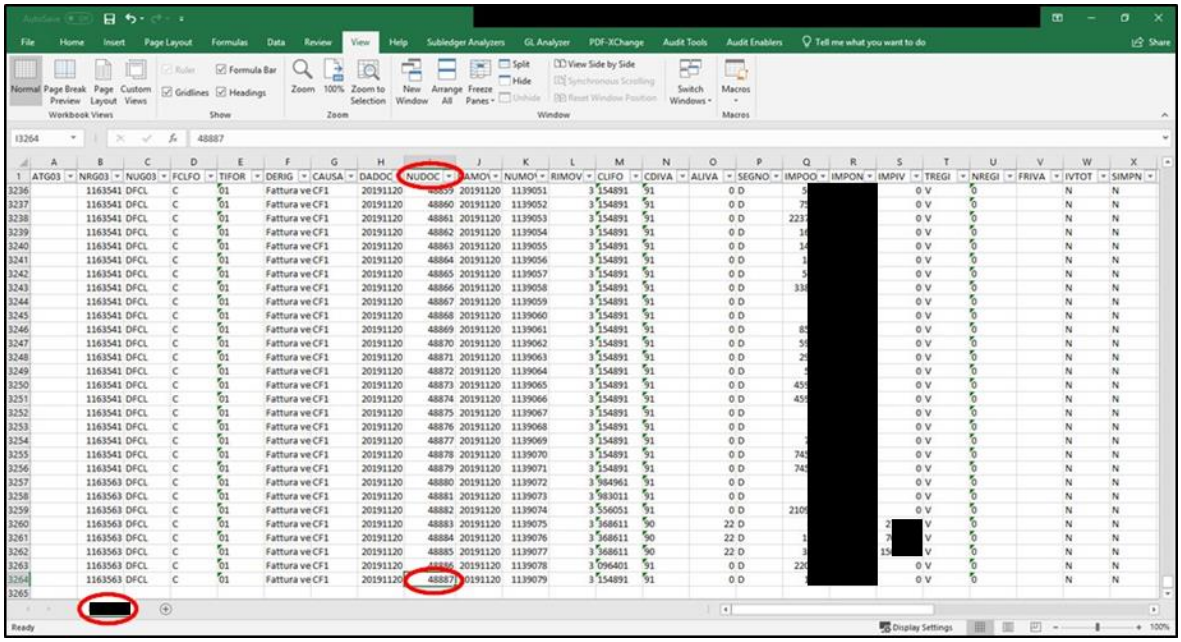


Figura 26 - Estrazione Excel lista documenti disponibili

Nella schermata in ***Figura 27*** dell'applicativo è mostrata la prima fattura disponibile con il numero "300141" (numero progressivo interno):

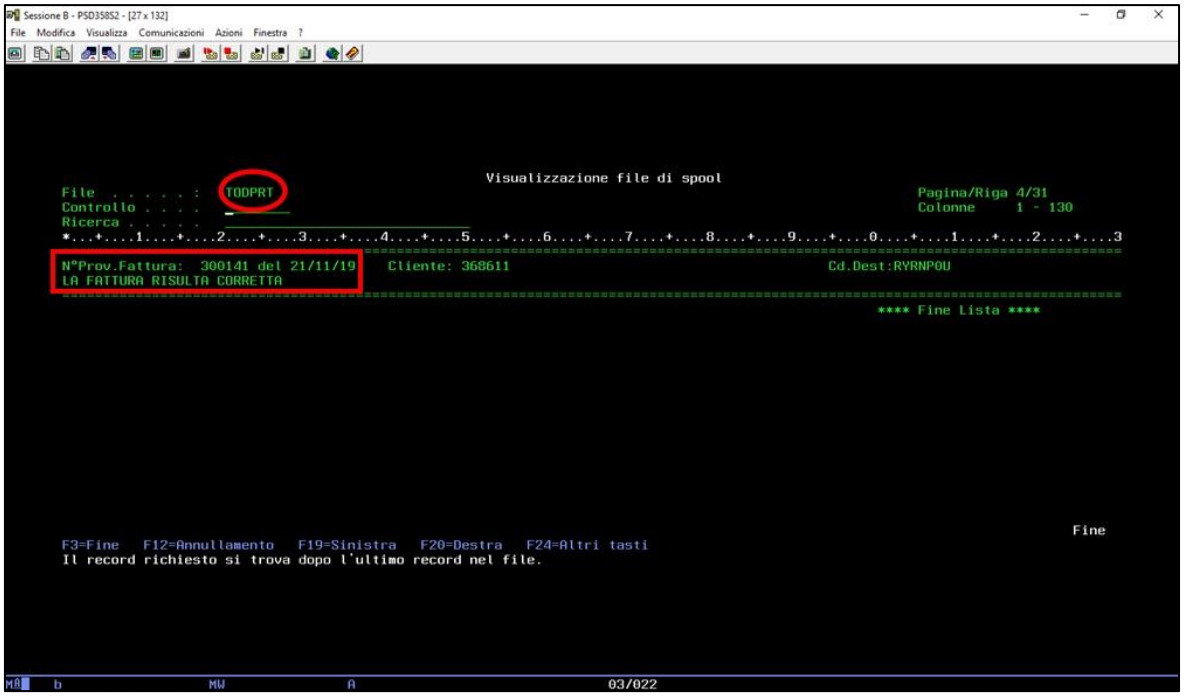


Figura 27 - Schermata applicativo "Visualizzazione fattura 300131 disponibile"

Tutte le fatture non ancora registrate sono dotate di un numero temporaneo (progressivo). Nella schermata in ***Figura 28*** è quindi stata selezionata la numero "300141" perché, come spiegato sopra, risulta la prima disponibile:

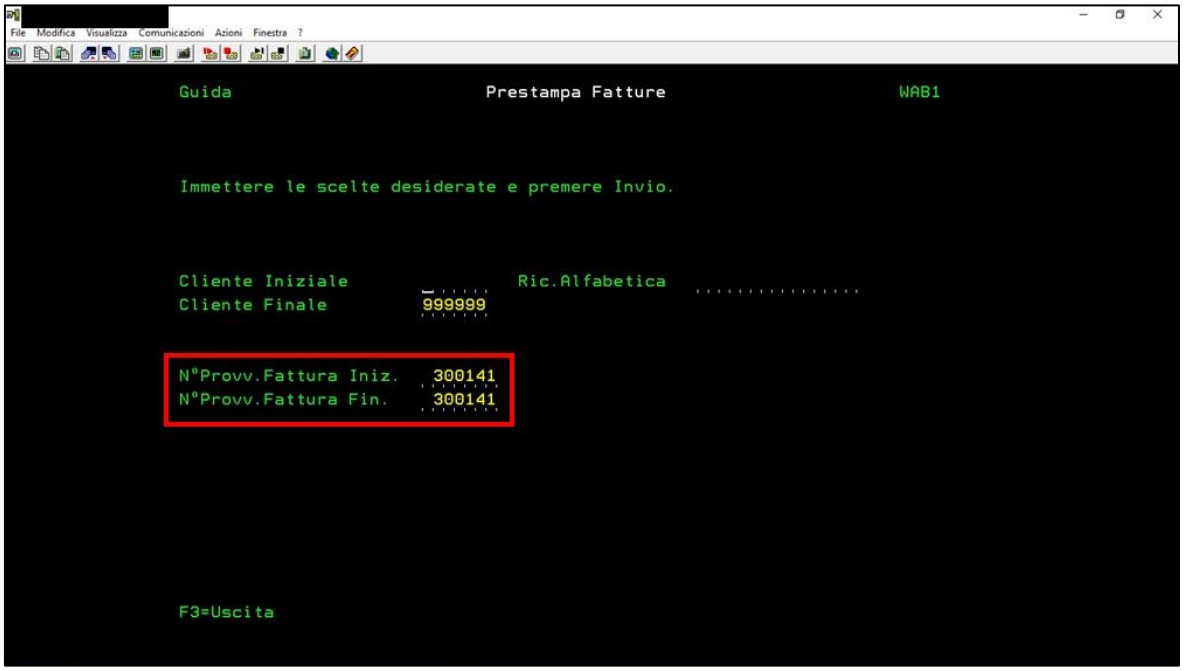


Figura 28 - Schermata "Prestampa Fattura 300141 Disponibili"

Per vedere tutti i dettagli della fattura, è stato stampato il documento "pre-fattura", che può essere visto nella schermata di stampa in ***Figura 29***:

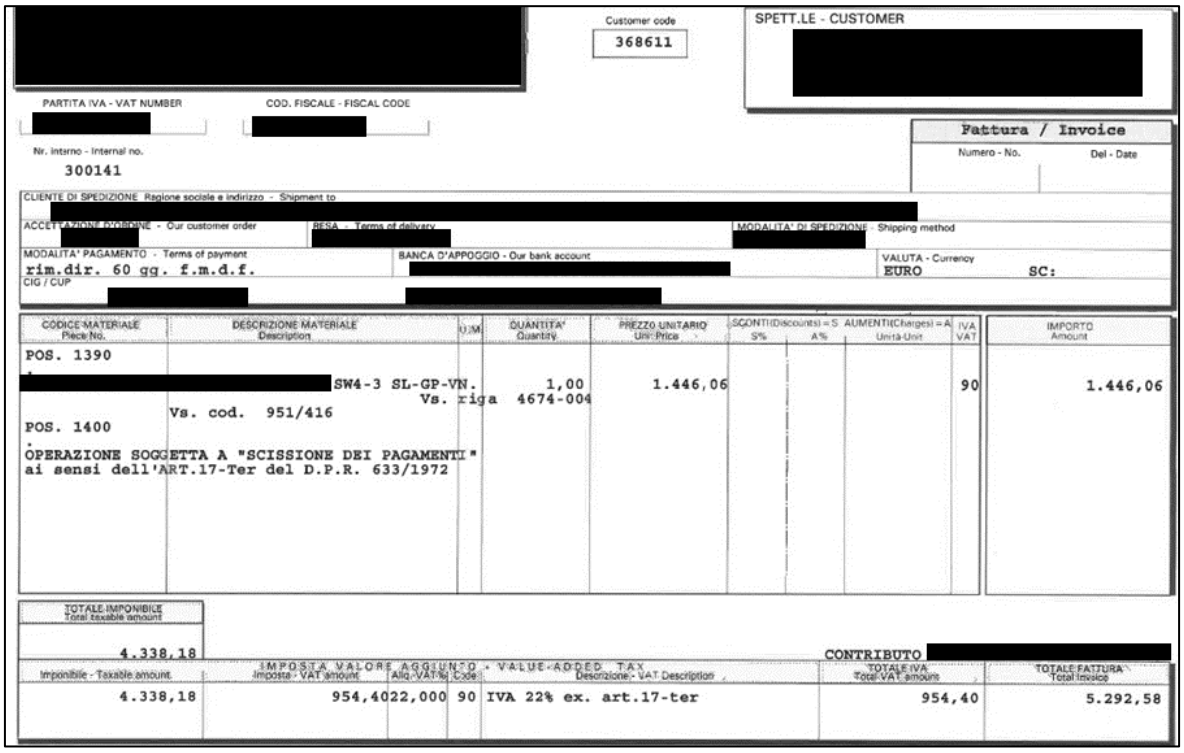


Figura 29 - Schermata prestampa Documento 300141

Per registrare la fattura, la Società X deve fare un caricamento massivo delle registrazioni contabili sull'applicativo in analisi. L'azienda ha quindi proceduto avviando questo caricamento massivo dei dati delle fatture (***Figura 30***):

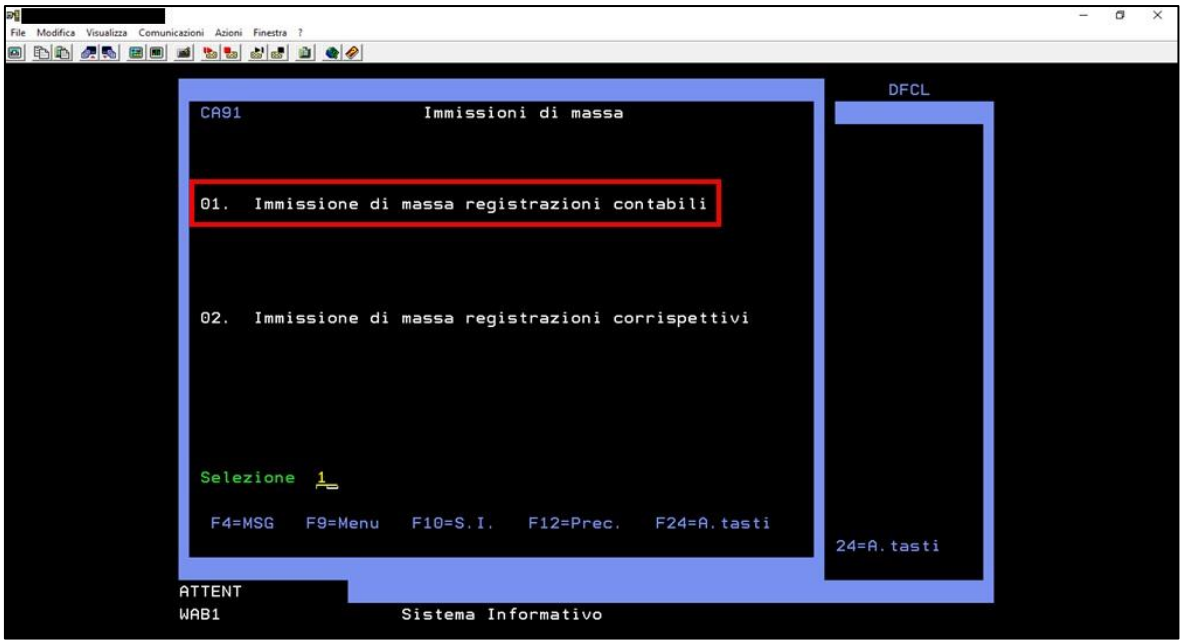


Figura 30 - Schermata "Immissioni di massa" fatture disponibili

Dopo il caricamento massivo, vengono mostrati dei documenti per confermare il risultato positivo dell'operazione. Come si può vedere nella schermata di stampa in ***Figura 31***, l'upload eseguito ha avuto un risultato positivo:

Figura 31 - Schermata visualizzazione conclusione coricamento documenti

Nelle schermate visibili nelle ***Figura 32-33***, la fattura risulta registrata correttamente nel sistema dell'applicativo, riportando gli stessi dettagli della fattura prestampata, con il numero di fattura 48888:

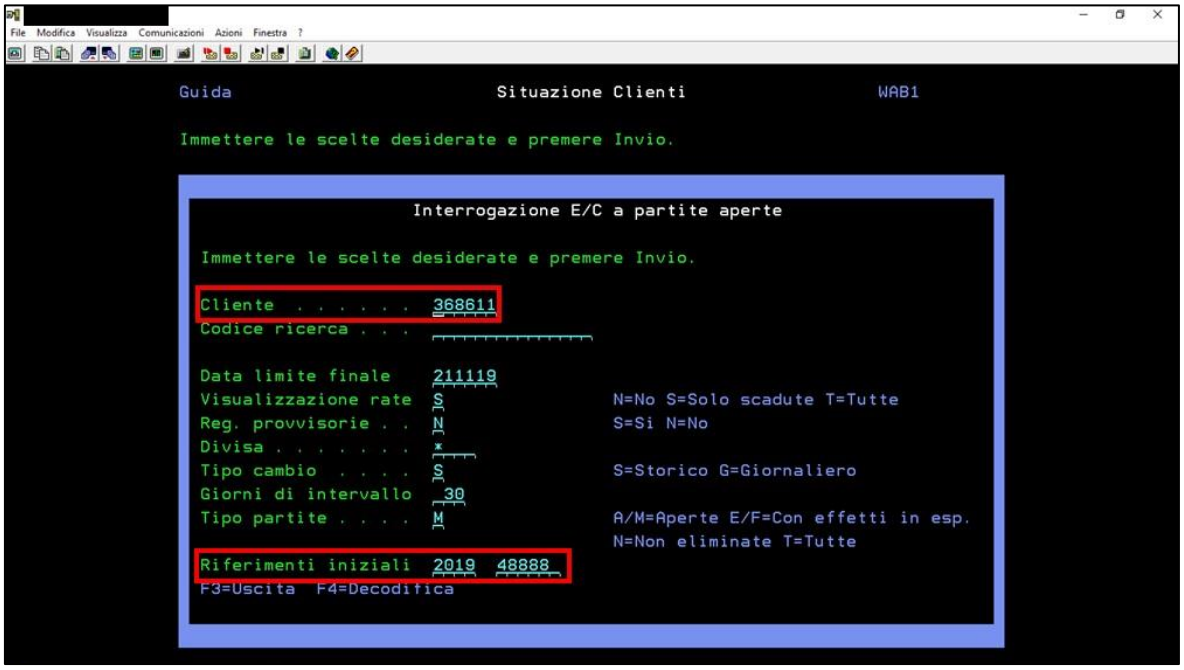


Figura 32- Schermata riepilogo fattura 48888

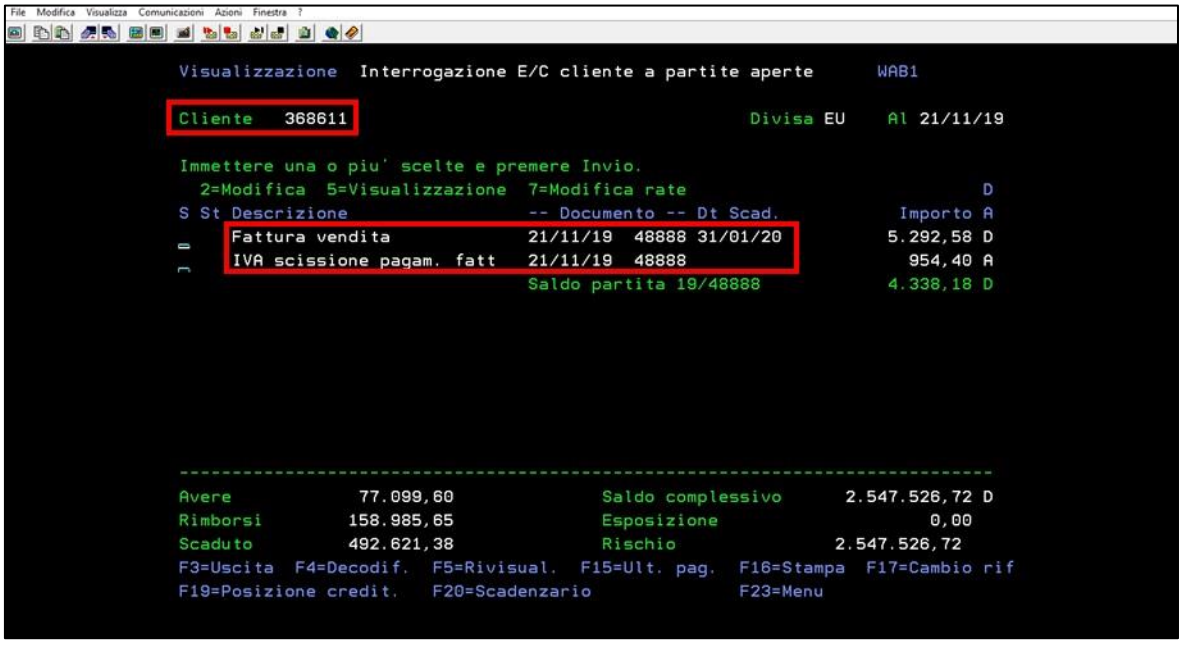


Figura 33 - Schermata riepilogo fattura 48888

La società X ha dunque terminato il "positive test" secondo le aspettative dello scenario predefinito.

La Società X ha poi provato a verificare il "negative test" andando a fatturare di nuovo il precedente articolo registrato. Guardando il menù, mostrato nella ***Figura 34***, in cui sono visibili tutte le possibili voci da fatturare (dalla voce "Coda di stampa"), le fatture registrate nei passi precedenti non sono più disponibili (non risultano indicate né al numero "48887" né al "48888"). Ciò significa che non è possibile rifatturare due volte lo stesso articolo.

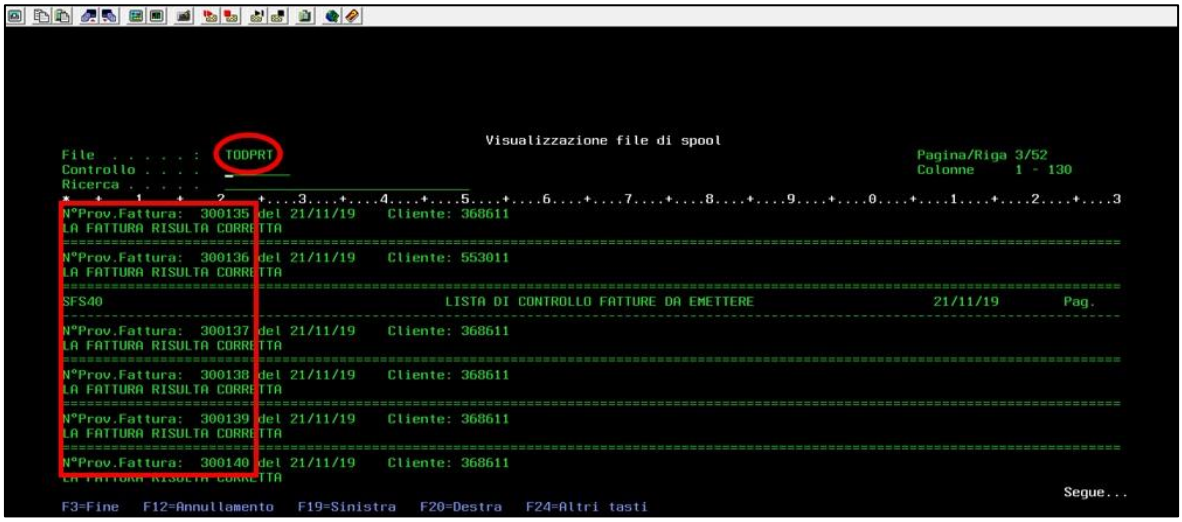


Figura 34 – Schermata "Codi di stampa"

Nell'effettuare questo controllo, è stato verificato che non sono state riportate alcune eccezioni rispetto al disegno delle strategie definite inizialmente; inoltre non sono stati individuati aspetti di configurabilità per cui sarebbe stato necessario richiedere specifiche analisi ai referenti della Società X hai fini di valutare che non fossero presenti anomalie nel sistema.

In conclusione, secondo la strategia descritta nel secondo capitolo, sono stati effettuati:

- Il "positive test", che è rappresentato dalla verifica della generazione della fattura per un determinato documento portata a termine con successo e senza anomalie;
- Il "negative test", verificando che il programma non permette di fatturare due volte lo stesso documento se risulta già essere precedentemente fatturato.

3.3.5 Test delle IPE

L'IPE si riferiscono, come già descritto nel capitolo due, a qualsiasi documento, elenco o insieme di informazioni di un'azienda. Quando l'azienda utilizza un IPE per ricavare informazioni contabili, è necessario che sia il più accurato e completo possibile perché, se durante l'estrazione dei rapporti alcuni dati vengono persi, questo potrebbe generare errori a cascata compromettendo l'integrità dei risultati. Supponiamo ad esempio il caso in cui i dati estratti vengono utilizzati come fonte per fare dei calcoli; se l'errore all'origine non fosse trascurabile, questo potrebbe aumentare nel tempo fino a raggiungere un risultato finale che si discosta da quello corretto di diversi ordini di grandezza.

L'obiettivo del controllo che descriveremo in questo paragrafo si concentra su questo problema. A tal fine, è quindi necessario verificare che lo strumento utilizzato dall'azienda estragga correttamente le informazioni e che queste corrispondano quindi ai dati di partenza contenuti nei database dell'azienda.

Andiamo quindi a testare:

1. La corrispondenza del numero di record nel rapporto dello strumento e nel database. (Completezza).
2. La corrispondenza delle informazioni fornite per ogni rapporto. (Accuratezza)
3. La corrispondenza della somma dei valori per i campi di interesse (Accuratezza)

Per realizzare questo controllo è necessario utilizzare un report dal tool aziendale della Società X e un report contenente i dati estratti direttamente dal database; nello specifico, per la descrizione che segue, è stato utilizzato un report dell'azienda contenente informazioni sul WIP del magazzino.

1. Completezza

Al fine di verificare la completezza è stato fatto un check sul numero totale di record presenti in entrambi i report. Per garantire che nessun record venga perso durante l'estrazione, il numero totale deve corrispondere sia per il report da tool che per l'estrazione del database.

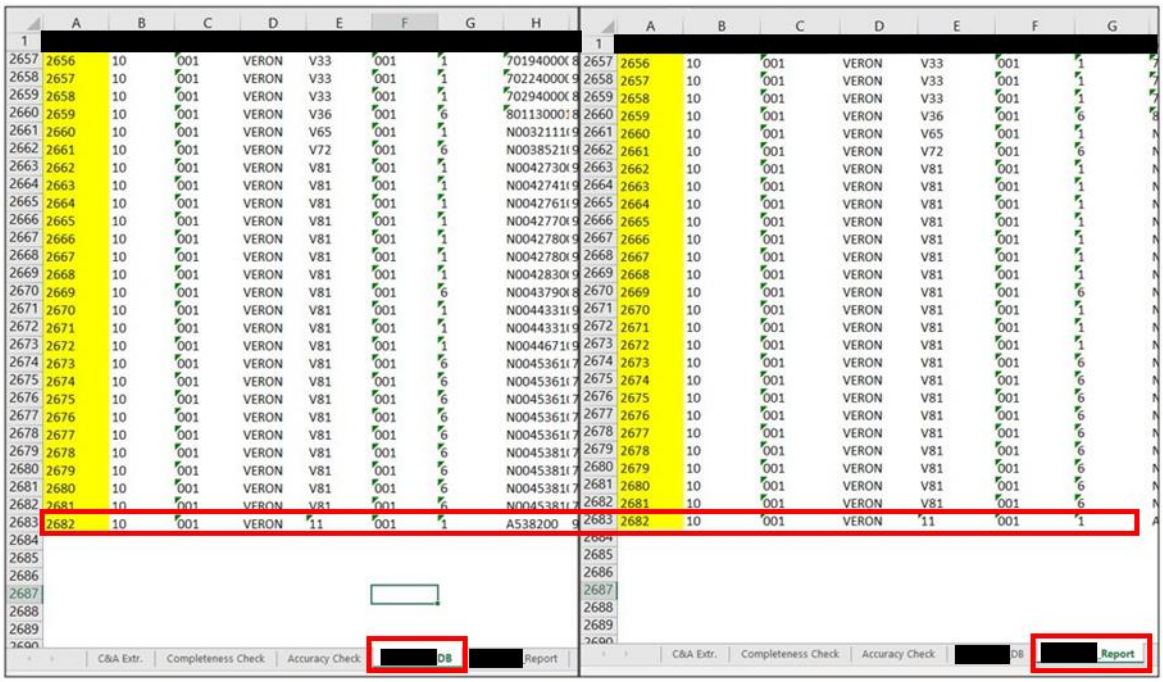
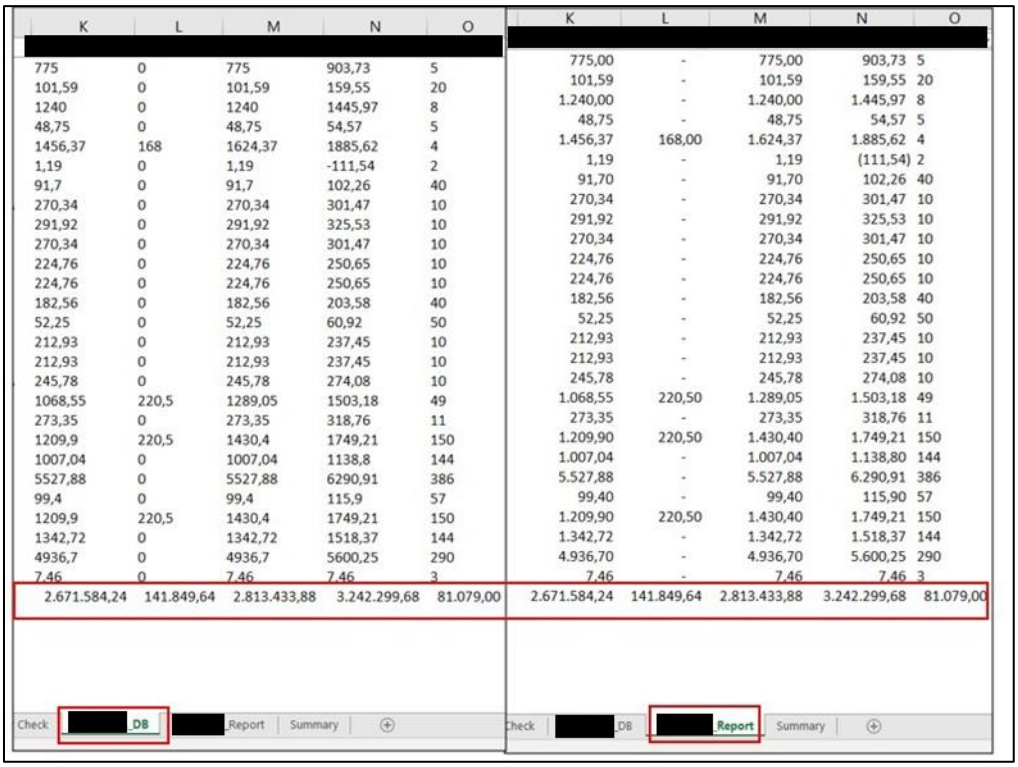


Figura 35 - Visualizzazione report estratti da Tool / Database

Come si può vedere nella ***Figura 35***, entrambi i rapporti contengono 2.682 record. Viene approvata la completezza del report poiché non risultano perdite di record.

2. Accuratezza

Per verificare l'accuratezza, abbiamo in primis controllato che i dati delle somme totali dei costi corrispondessero. La legenda qui sotto aiuta a capire la tabella.
Le voci da controllare sono i valori relativi alle diverse tipologie di WIP (Vedi ***Figura 36***, da sinistra a destra WIP del costo del materiale, WIP del costo del lavoro diretto ecc, WIP Standard e WIP Prime) e poi la commessa (Vedi ***Figura 36***, la colonna "0"). Dopo di che è stata calcolata la somma totale di questi costi includendo tutti i record della tabella.



K	L	M	N	O
775	0	775	903,73	5
101,59	0	101,59	159,55	20
1240	0	1240	1445,97	8
48,75	0	48,75	54,57	5
1456,37	168	1624,37	1885,62	4
1,19	0	1,19	-111,54	2
91,7	0	91,7	102,26	40
270,34	0	270,34	301,47	10
291,92	0	291,92	325,53	10
270,34	0	270,34	301,47	10
224,76	0	224,76	250,65	10
224,76	0	224,76	250,65	10
182,56	0	182,56	203,58	40
52,25	0	52,25	60,92	50
212,93	0	212,93	237,45	10
212,93	0	212,93	237,45	10
245,78	0	245,78	274,08	10
1068,55	220,5	1289,05	1503,18	49
273,35	0	273,35	318,76	11
1209,9	220,5	1430,4	1749,21	150
1007,04	0	1007,04	1138,8	144
5527,88	0	5527,88	6290,91	386
99,4	0	99,4	115,9	57
1209,9	220,5	1430,4	1749,21	150
1342,72	0	1342,72	1518,37	144
4936,7	0	4936,7	5600,25	290
7,46	0	7,46	7,46	3
2.671.584,24	141.849,64	2.813.433,88	3.242.299,68	81.079,00

K	L	M	N	O
775,00	-	775,00	903,73	5
101,59	-	101,59	159,55	20
1.240,00	-	1.240,00	1.445,97	8
48,75	-	48,75	54,57	5
1.456,37	168,00	1.624,37	1.885,62	4
1,19	-	1,19	(111,54)	2
91,70	-	91,70	102,26	40
270,34	-	270,34	301,47	10
291,92	-	291,92	325,53	10
270,34	-	270,34	301,47	10
224,76	-	224,76	250,65	10
224,76	-	224,76	250,65	10
182,56	-	182,56	203,58	40
52,25	-	52,25	60,92	50
212,93	-	212,93	237,45	10
212,93	-	212,93	237,45	10
245,78	-	245,78	274,08	10
1.068,55	220,50	1.289,05	1.503,18	49
273,35	-	273,35	318,76	11
1.209,90	220,50	1.430,40	1.749,21	150
1.007,04	-	1.007,04	1.138,80	144
5.527,88	-	5.527,88	6.290,91	386
99,40	-	99,40	115,90	57
1.209,90	220,50	1.430,40	1.749,21	150
1.342,72	-	1.342,72	1.518,37	144
4.936,70	-	4.936,70	5.600,25	290
7,46	-	7,46	7,46	3
2.671.584,24	141.849,64	2.813.433,88	3.242.299,68	81.079,00

Figura 36 - Tabella WIP commesse

Come si può vedere dalla ***Figura 37***, i costi per tutti gli articoli corrispondono alla seconda cifra decimale. Per un ulteriore controllo di precisione, le somme totali della tabella estratte dallo strumento sono state confrontate con i dati inseriti direttamente nel sistema.

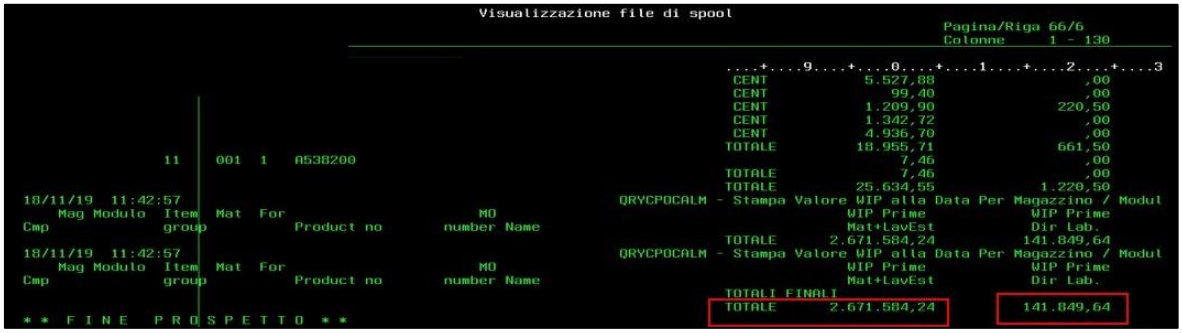
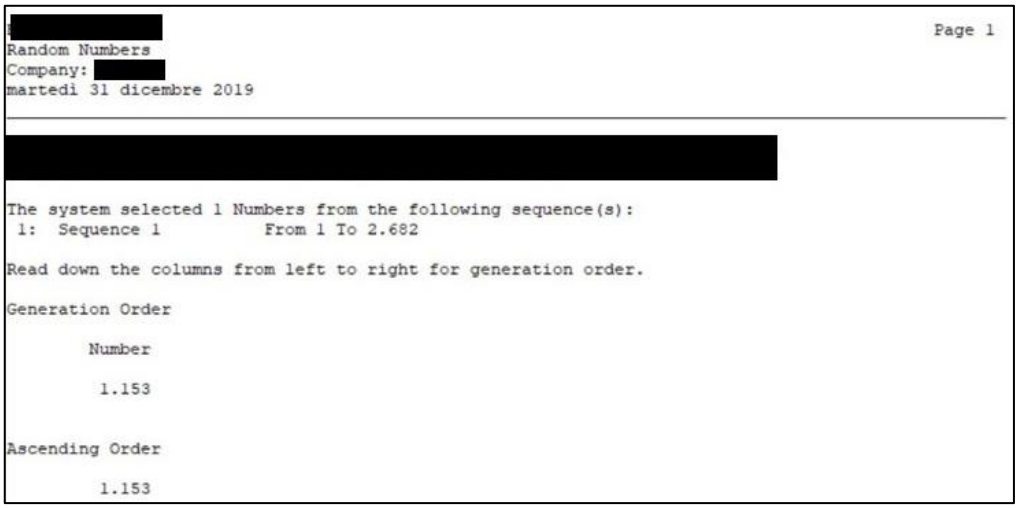


Figura 37 – Schermata applicativo Visualizzazione costo totale

L'ultimo controllo di accuratezza consiste nel campionare un singolo record usando un metodo casuale. Una volta scelto il record, questo viene isolato da entrambe le tabelle e si controlla che tutti i valori di dei campi di ciascuna colonna siano uguali.

Il record 1.153 è stato scelto per questo controllo (vedi ***Figura 38***).



[redacted] Page 1
Random Numbers
Company: [redacted]
martedi 31 dicembre 2019

[redacted]

The system selected 1 Numbers from the following sequence(s):
1: Sequence 1 From 1 To 2.682

Read down the columns from left to right for generation order.

Generation Order

Number

1.153

Ascending Order

1.153

Figura 38 - Schermata esito campionamento casuale

Come si può vedere nella ***Figura 39***, entrambi i rapporti mostrano lo stesso valore.

DB

#	PDCONO	VHWHLO	MMRESP	MMITGR	MMACRF	MMITTY	VHPRNO	VHMFNO	MMITDS	WIPMAT	WIPLAB	WIPPRI	PDTODF	VHORQT	VHWHST	VHWHHS	VHSLDT
1153	10	001	BRAKE	06	001	1	RV/048340	9460409	REV.DOPPI	29,17	23,36	52,53	55,53	5	60	70	20190920

Report

#	PDCONO	VHWHLO	MMRESP	MMITGR	MMACRF	MMITTY	VHPRNO	VHMFNO	MMITDS	WIPMAT	WIPLAB	WIPPRI	PDTODF	VHORQT	VHWHST	VHWHHS	VHSLDT
1153	10	001	BRAKE	06	001	1	RV/048340	9460409	REV.DOPPI	29,17	23,36	52,53	55,53	5	60	70	20190920

Check of Accuracy

#	PDCONO	VHWHLO	MMRESP	MMITGR	MMACRF	MMITTY	VHPRNO	VHMFNO	MMITDS	WIPMAT	WIPLAB	WIPPRI	PDTODF	VHORQT	VHWHST	VHWHHS	VHSLDT
TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE

Figura 39 - Recap calcolo costo dal report Tool / Database

Poiché entrambe le condizioni di completezza e accuratezza sono state verificate, il test è di conseguenza efficace, e si può concludere che il rapporto è affidabile e il rischio che i dati utilizzati non siano completi è correttamente mitigato.

3.3.6 Conclusione del progetto di revisione dei sistemi informativi

Dopo avere quindi terminato tutti i test relativi ai controlli ITGC, ITAC e i test sulle IPE si è giunti quindi alla conclusione del ciclo di audit IT della Società X. La time line, che ha scandito l'esecuzione di questi test, per rispettare le scadenze dettate dalle normative di chiusura del bilancio contabili, ha visto procedere in parallelo questi vari test dei controlli in base alle informazioni che sono state man mano raccolte tramite il materiale ricevuto dai referenti dell'azienda cliente.

Al termine di tutte le analisi non sono state riportate particolari anomalie nel funzionamento degli applicativi e dell'infrastruttura IT in revisione per Società X, per cui nessuno controllo testato è stato considerato come "ineffective". Abbiamo quindi valutato il sistema informativo dell'azienda come "Support" al fine di effettuare una corretta revisione del bilancio.

In seguito alla valutazione del sistema IT, si sono riporti gli esiti dei test anche al team della Funzione IT della Società X; abbiamo quindi definito loro un rapporto di tutti gli aspetti analizzati, sia di quei processi che hanno confermato il corretto funzionamento al disegno del controllo, sia quelli per cui abbiamo individuato possibili spunti di miglioramento che la Società X potrebbe adottare al fine di mitigare in maniera più accurata i relativi rischi IT.

Una volta comunicati questi risultati, si può definire conclusa l'attività del team di audit IT, per ciclo di audit dell'azienda cliente.

La vera conclusione del progetto di revisione dell'azienda termina invece, come descritto nel secondo capitolo, con la stesura della lettera di opinion firmata dal partner di EY e mandata, in seguito alla conclusione da parte dei colleghi revisori delle loro analisi di contabilità finanziaria, agli amministratori della Società X.

Capitolo 4

4.1 La nuova direzione dell'Audit

La professione dell'Internal Audit non ha mai dovuto affrontare la necessità di dover innovare e reinventarsi fino a quest'ultimo decennio. Come visto, sin dalla nascita e lungo tutto il suo percorso, lo sviluppo di vari framework e la redazione di normative hanno contribuito ad un continuo miglioramento di questa professione in termini di capacità e analisi dei dati.

Oggi però l'avvento di nuove tecnologie digitali ha indirizzato tutte le organizzazioni nel dover riadattarsi per poter affrontare una nuova evoluzione che impatterà dal punto di vista della definizione della strategia, dei processi operativi e i nuovi rischi informatici ad essi legati.

Il cambiamento apportato dalla quarta rivoluzione industriale, con l'avvento delle nuove tecnologie e della digitalizzazione, ha fatto sì che il mondo del business stia cambiando in tutte le sue forme e figure interne. Le società di consulenza stanno così cavalcando la spinta che viene dall'esterno, adottando nuovi modelli di business che prevedono l'integrazione di piattaforme digitali in modo da permettere all'attività di auditing di poter adottare nuovi approcci per controllare i rischi e testare i controlli che nasceranno con le nuove tecnologie dirompenti.

La natura interconnessa delle operazioni guidate dall'industria 4.0 e il ritmo della trasformazione digitale ha infatti fatto sì che gli attacchi informatici possano avere un effetto più ampio all'interno delle organizzazioni. Bisognerà infatti bilanciare l'attenzione delle imprese affinché possano affrontare, da un lato il panorama delle minacce esterne e i rischi reali informatici, tipicamente trascurati, che si vanno a creare all'interno delle aziende che utilizzano sempre più tecnologie intelligenti e interconnesse, dall'altro proseguire nel processo di innovazione, trasformazione e modernizzazione attuando strategie o decisioni aziendali tattiche che potrebbero comportare tali rischi.

4.2 Industria 4.0 e rischio cyber

Le tecnologie dell'Industria 4.0 che abilitano le imprese manifatturiere e reti di fornitura digitali coinvolgono l'integrazione di informazioni digitali da molte fonti e luoghi diversi per guidare l'atto fisico della produzione e della distribuzione. Questa integrazione di tecnologia dell'informazione e tecnologia operativa è caratterizzata da uno spostamento verso una connessione fisico-digitale-fisico.

L'industria 4.0 combina l'Internet of Things (IoT) e le tecnologie fisiche e digitali pertinenti, tra cui l'analisi, la produzione additiva, la robotica, il calcolo ad alte prestazioni, l'intelligenza artificiale e le tecnologie cognitive, i materiali avanzati e la realtà aumentata, per completare quel ciclo e digitalizzare le operazioni aziendali.

Si preannuncia una nuova era di produzione connessa e intelligente, reti di fornitura reattive, prodotti e servizi su misura. Attraverso l'uso di tecnologie intelligenti e autonome, l'Industria 4.0 si sforza di sposare il mondo digitale con l'azione fisica per guidare le smart factory e consentire la produzione avanzata.

Il concetto di Industria 4.0 incorpora ed estende l'IoT nel contesto del mondo fisico integrando dei salti fisico-digitale e digitale-fisico che sono in qualche modo unici per la produzione e la catena di approvvigionamento e processi di rete. È il salto dal digitale al fisico, dalle tecnologie digitali connesse alla creazione di un oggetto fisico, che costituisce l'essenza dell'industria 4.0 come base dell'impresa manifatturiera digitale e della rete di fornitura digitale.

Tutti questi cambiamenti e miglioramenti guidati dalle capacità digitali lungo la catena di produzione di fornitura portano con sé nuovi rischi informatici per i quali l'industria è impreparata. Occorre quindi sviluppare un approccio strategico completamente integrato al rischio informatico a pari passo con l'adozione della Operation Technology (OT) e l'Information Technology (IT), vere forze guida dell'Industria 4.0.

La quarta rivoluzione industriale ha portato con sé un nuovo rischio operativo per le smart factory e per le Digital Supply Chain (DSC): il rischio cyber.

Le reti interconnesse portate dall'Industria 4.0 e il ritmo della trasformazione digitale fanno sì che i cyberattacchi possano avere effetti molto più estesi che mai, e i produttori e le loro reti di fornitura potrebbero non essere preparati a tali rischi. Per affrontare adeguatamente il rischio informatico nell'era dell'Industria 4.0, le strategie di cybersecurity dovrebbero essere sicure, vigili e resilienti, oltre che pienamente integrate nella strategia organizzativa e informatica fin dall'inizio.

Tabella 9 – Industry 4.0: Cyber Security e Digital Supply Chain (DSC)

Digital Supply Chain (DSC)	CARATTERISTICHE	IMPERATIVI CYBER	OBIETTIVI
	Sicuro, Vigile, Resiliente	Condivisione di Dati	Garantire l'integrità dei sistemi in modo che non si possa accedere a dati di proprietà e privati.
	Sicuro, Vigile, Resiliente	Rete di Fornitori	Affidabilità dei processi dei fornitori terzi.

L'avvento dell'industria 4.0 ha fatto sì che queste minacce si espandessero radicalmente, così che dovranno essere considerati e affrontati dei nuovi rischi. In altre parole, i cambiamenti portati da questa nuova rivoluzione industriale impattano direttamente la gestione di una strategia di rischio informatico sicura, vigile e resiliente che deve adattarsi ai nuovi rischi e alle minacce informatiche diventate sempre più grandi e potenzialmente più estese nell'organizzazione.

Per contrastare questi rischi bisogna quindi agire, così che non vengano affrontati solo al termine del processo strategico, ma che si vadano a considerare le tematiche sulla sicurezza informatica come parte integrante del processo decisionale di definizione strategica, del design e delle operazioni, per qualsiasi iniziativa guidata da un sistema interconnesso.

4.2.1 I cambiamenti dell'industria 4.0 sulle DSC

Le nuove tecnologie importate dall'Industria 4.0, introducono una nuova evoluzione alla struttura lineare della catena del valore, dalla produzione alla distribuzione.

I risultati di business che possono emergere introducendo piattaforme e dispositivi intelligenti e connessi in tutto l'ecosistema, permettono di avere una supply chain digitale in grado di catturare informazioni da ogni punto della catena del valore. Tutto ciò permette di ottenere una migliore gestione del flusso di materiali e merci, un uso più efficiente delle risorse e delle forniture per soddisfare più adeguatamente le esigenze dei clienti.

Nonostante ciò, la crescente interconnessione della Digital Supply Chain porta con sé anche debolezze informatiche che dovrebbero essere adeguatamente pianificate e prese in considerazione in ogni fase della progettazione, per prevenire rischi significativi.

L'evoluzione rete di fornitura digitale consentirà, secondo le aspettative, di creare una rete che permetta la determinazione in tempo reale e dinamica dei prezzi dei materiali o delle merci in base alla domanda degli acquirenti rispetto all'offerta disponibile. Ma una rete agile e reattiva di questa natura è resa possibile solo dalla condivisione di dati aperti da parte di tutti i partecipanti alla rete di fornitura, il che crea un ostacolo significativo: sarà probabilmente difficile trovare un equilibrio tra permettere la trasparenza di alcuni dati e mantenere la sicurezza per altre informazioni.

Tutto ciò porterebbe le organizzazioni a voler considerare dei modi per proteggere informazioni sensibili per impedire agli utenti non autorizzati di accedervi attraverso la rete.

Allo stesso tempo le società avrebbero necessità di mantenere maggiori protezioni in tutti i processi di supporto, come l'accettazione del fornitore, la condivisione delle informazioni e l'accesso al sistema. Questi processi possono essere limitati al singolo accesso, ma possono anche potenzialmente essere strumenti di collegamento verso altre informazioni interne.

Questo duplice interesse si riflette direttamente sulla gestione del rischio di terzi. Per analizzare i rischi informatici delle DSC interconnesse sono identificate due aree principali influenzate dall'aumento della connettività della catena di fornitura: la condivisione dei dati e l'esposizione a rischio dei processi dei fornitori esterni.

4.2.2 L'impatto del cyber risk sui sistemi industriali embedded e ICS

Le smart factory così come le interconnessioni delle digital supply chain introducono nuovi vettori di rischio che aumentano e si diversificano anche in modo esponenziale: un esempio lo sono i rischi associati ai sistemi embedded life-critical che i produttori possono implementare nella produzione, sia direttamente che indirettamente.

Con il termine "sistemi embedded life-critical" sono considerati quei sistemi per i quali quasi tutti i processi sono connessi, sia quelli dei dispositivi all'interno dell'organizzazione in un sistema automatizzato, sia quelli situati in remoto presso i produttori terzi, in più, dovrebbero essere considerati un rischio, anche quei dispositivi che toccano solo marginalmente o indirettamente il processo di produzione.

Questo aumento del rischio intrinseco nei processi, guidato dall'industria 4.0, ha portato alla necessità di un cambiamento fondamentale nei modi in cui la sicurezza deve essere gestita.

Dal punto di vista operativo, i moderni sistemi di controllo industriali (ICS) hanno permesso di implementare siti non presidiati mantenendo un'alta efficienza e il controllo delle risorse. Tutto ciò può essere raggiunto utilizzando sistemi che collegano la pianificazione delle risorse aziendali, la produzione e i sistemi di controllo e acquisizione dati: questi sistemi connessi possono spesso snellire i processi e rendere le cose più facili ed efficienti.

I miglioramenti che si introducono sull'efficienza operativa impattano però negativamente dal punto di vista della sicurezza: l'aumento del networking e l'uso

di prodotti commerciali off-the-shelf (COTS) negli ICS introduce una varietà di punti di esposizione che potrebbero essere terreno di cyber attacchi.

Dal punto di vista tecnologico le soluzioni di sicurezza IT convenzionali non sono adatte alle reti industriali, che sono caratterizzati da un'alta tolleranza di falsi positivi, un consumo delle risorse elevato e una connessione costante a Internet, elementi che non si adattano ai moderni sistemi ICS.

Installare protezioni per endpoint di sicurezza IT convenzionali in un ambiente ICS può addirittura costituire un pericolo e portare all'interruzione dei processi industriali, ecco perché l'attenzione della sicurezza ICS si concentra sul processo industriale.

Pertanto, gli obiettivi nelle smart factory si concentrano principalmente sulla disponibilità e l'integrità del processo fisico piuttosto che sulla riservatezza delle informazioni.

Tabella 10 - Approccio alla Cyber Security delle Smart Factory

Smart Factory	CARATTERISTICHE	IMPERATIVI CYBER	OBIETTIVI
	Vigile, Resiliente	Resilienza ed efficienza della produzione e dei processi	Garantire la produzione continua e il recovery dei sistemi critici
	Sicura, Resiliente	Operabilità, affidabilità e integrità dei sistemi	Supportare l'uso di più fornitori e versioni di software
	Vigile, Resiliente	Efficienza e riduzione dei costi	Ridurre i costi operativi e aumentare la flessibilità attraverso la diagnostica del sito in remoto

Ogni organizzazione dovrebbe adattarsi all'ecosistema industriale nel modo più adatto alle proprie esigenze. Non esiste una semplice correzione o singolo prodotto o patch che un'organizzazione possa applicare per affrontare i rischi e le minacce informatiche presentati dall'Industria 4.0.

L'ampiezza dei rischi richiede un approccio sicuro, vigile e resiliente per comprendere i pericoli e affrontare le minacce:

- Sicuro: adottare un approccio misurato e basato sul rischio a ciò che è sicuro e a come proteggerlo.

- Vigile: monitorare continuamente sistemi, reti, dispositivi, personale e ambiente per possibili minacce. L'intelligenza artificiale in tempo reale e i metodi previsionali sono spesso necessari per comprendere le azioni dannose e identificare rapidamente le minacce introdotte dalla moltitudine di nuovi dispositivi connessi.

- Resiliente: capacità in termini di efficienza, tempi di risposta e rapidità con cui si interviene per correggere tutti gli effetti generati da un possibile incidente.

Più il settore si muove per catturare il valore aziendale fornito dalle innovazioni introdotte con l'Industria 4.0, più cresce la necessità di affrontare il panorama del rischio informatico con una risposta sicura, vigile e resiliente.

4.3 Rischio cyber e audit interno

Le minacce degli attacchi informatici sono diventate così significative e in continua crescita che le organizzazioni hanno avuto la necessità di avere una nuova prospettiva di audit interno che sia utile a comprendere e valutare le capacità della gestione dei rischi cyber.

Per far fronte a queste minacce le business unit e la funzione IT integrano la gestione del rischio informatico nel processo decisionale e nelle operazioni quotidiane costituendo una prima linea di difesa delle organizzazioni.

Inoltre, le figure di controllo nella gestione dei rischi IT che stabiliscono la governance, la supervisione e monitorano le operazioni di sicurezza prendendo misure necessarie, costituiscono quella che è definita come seconda linea di difesa.

Oltre queste linee, sempre più spesso molte aziende riconoscono la necessità di una terza linea di revisione, indipendente dalla difesa informatica e dalle misure di sicurezza e delle prestazioni, identificata con la funzione dell'audit interno.

L'audit interno dovrebbe svolgere un ruolo fondamentale nella valutazione e nell'individuazione delle opportunità per rafforzare la sicurezza delle imprese. Allo

stesso tempo, l'audit interno ha il dovere di informare il comitato di audit e il consiglio di amministrazione che i controlli di cui sono responsabili sono in atto e funzionano correttamente.

Per una analisi iniziale, un passo efficace per l'audit interno consiste nel condurre una valutazione del rischio informatico e la relativa diffusione dei risultati, attraverso una sintesi concisa per il comitato di audit e il consiglio di amministrazione, che orienterà la definizione di un piano di audit interno pluriennale sulla cyber security.

4.4 L'approccio di valutazione della cybersecurity:

L'audit interno ha un ruolo chiave nell'aiutare le organizzazioni nella continua battaglia della gestione delle minacce informatiche, sia fornendo una valutazione indipendente di controlli esistenti e necessari, sia aiutando il comitato di controllo e il consiglio a capire e ad affrontare i diversi rischi del mondo digitale.

L'attività di revisione segue una serie di procedure guida che aiutano i team di audit ad ottenere una comprensione ideale dei rischi cyber che l'entità aziendale sotto analisi deve affrontare a causa delle minacce informatiche.

Per lo svolgimento dell'attività di questa attività di auditing viene utilizzato un modulo al fine di facilitare la comprensione dei rischi aziendali e di capire come l'organizzazione sta rispondendo a tali rischi.

In ambito cybersecurity, l'attività dell'auditing sta nel definire l'insieme di tecnologie, processi e pratiche utili ai fini di proteggere le reti, i sistemi host, le applicazioni e le informazioni e sostenere un sistema resiliente per rispondere agli impatti di un attacco informatico.

Per stimare il rischio cyber si possono considerare le probabilità che queste tecnologie, processi e pratiche possano essere aggirate (permettendo quindi l'accesso e non autorizzato a informazioni protette e sensibili, con la possibilità di modificarle o cancellarle) impattando sull'accuratezza e sull' integrità dei sistemi di elaborazione.

L'approccio standard dell'audit in ottica cybersecurity impone in primis di eseguire una procedura di valutazione dei rischi sufficiente a fornire una base ragionevole per identificare e valutare i rischi di imprecisioni rilevanti per il bilancio, siano essi dovuti a frodi o errori così da poter poi progettare ed eseguire ulteriori procedure di revisione per rispondere a tali rischi.

Si segue quindi il seguente workflow di analisi:

- Comprensione dell'entità e dell'ambiente in cui opera per identificare i fattori di rischio;
- Definizione dei rischi, siano essi intrinseci, o rivelanti ai fini del bilancio;
- Progettazione e implementazione di risposte appropriate per affrontare i rischi identificati.

4.4.1 Comprensione dei rischi cyber

Nell'ambito della comprensione dell'attività, si valutano i rischi aziendali rilevanti che possono dar luogo a imprecisioni nel bilancio. Poiché gli incidenti informatici che vengono segnalati sono in continuo aumento, occorre considerare la probabilità che un attacco informatico determini effettivamente inesattezze nel bilancio.

Per una corretta comprensione occorre sviluppare una visione completa dei rischi informatici attraverso indagini, osservazioni e altre procedure di valutazione del rischio. Diventare più consapevoli dei rischi informatici e della natura dei recenti incidenti informatici che interessano il settore del cliente può essere utile per effettuare valutazioni del rischio.

Ai fini di effettuare una valutazione preliminare per comprendere l'esposizione a rischi informatici a cui una qualsiasi società è soggetta, vengono considerati i seguenti fattori:

- l'utilizzo dell'infrastruttura IT per archiviare informazioni critiche per il funzionamento delle sue attività o utili a massimizzare un vantaggio sul mercato;

- l'utilizzo di complessi sistemi di controllo industriali ICS;
- la dipendenza dalla connettività Internet per sostenere le operazioni commerciali;
- l'ampiezza del canale di venditori e fornitori terzi di servizi che hanno sistemi interconnessi;
- le possibili violazioni relative al settore in cui opera che determinano un rilevante impatto sulla società.

Per comprendere quale sia l'esposizione dell'entità e il suo approccio alla cyber security occorre quindi:

- esaminare le informazioni chiave e i rapporti di gestione relativi alle minacce informatiche e alle misure di sicurezza;
- interrogare il management delle funzioni IT, operation, finanza, legale e altri dipartimenti interessati sulla conoscenza dei programmi di cybersecurity societari;
- interrogare il personale direttivo chiave per determinare se sono a conoscenza di eventuali attacchi o violazioni informatiche e la natura di tali attacchi;
- documentare le informazioni chiave e i rapporti di gestione relativi alla sicurezza informatica che vengono presentati alla direzione esecutiva e/o al consiglio di amministrazione.

4.4.2 Definizione dei potenziali rischi cyber

Di seguito, sono definiti i principali rischi cyber che possono essere oggetto di analisi.

Tra i principali rischi informatici spesso evidenziati troviamo il rischio legato agli accessi degli account privilegiati.

Gli account privilegiati hanno infatti molti più grant o accessi rispetto ad una utenza usuale; questi privilegi sono dovuti alle possibili attribuzioni di responsabilità amministrative, del sistema di sicurezza o di configurabilità del supporto o applicativo.

Alcuni esempi sono l'esecuzione di attività di gestione delle utenze (creazione o modifica dell'utenza), oppure quelle attività di amministrazione dei database che permettono di attuare modifiche ai database stessi e alle loro strutture sottostanti, o anche quelle attività di modifiche sui parametri di elaborazioni dei sistemi e sulle variabili chiavi all'interno dei sistemi finanziari.

Oltre questa tipologia di rischio, un'attività che deve essere soggetta a un continuo monitoraggio è quella legata al programma di gestione degli incident.

Ancor prima di adottare un piano di Audit IT, le società monitoravano i ripetuti tentativi di log-in falliti come un modo per identificare un possibile attacco agli accessi del sistema, mentre tutti i log-in riusciti con successo, così come le attività in corso sulla rete, non erano soggetti al monitoraggio.

Oggi però gli attacchi agli accessi del sistema sono diventati molto più sofisticati e sottili nel loro approccio e di conseguenza, il tipo di monitoraggio richiesto per rilevare attività insolite o non autorizzate ha ampliato il suo specchio di ricerca.

Tale monitoraggio richiede quindi diversi approcci e strumenti per registrare essenzialmente tutte le attività di rete e monitorare i dati per un comportamento insolito o sospetto, ed anche competenze speciali per capire cosa cercare e come indagare sulle anomalie identificate.

Esempi del tipo di monitoraggio che le società possono eseguire includono la correlazione di eventi insoliti o sospetti che si verificano sul sistema così come il monitoraggio dell'accesso a determinate risorse ad alto rischio per garantire che vi accedano solo gli individui che ne hanno bisogno.

Un'ulteriore attività di controllo è legata alla gestione dei rischi legati al fornitore; gli attacchi informatici possono infatti essere indirizzati contro il sistema IT della società esterna che, in un'ottica di interconnessione della catena di fornitura, rendono necessaria definizione di requisiti utile al controllo dell'ambiente IT dei terzi.

Difatti per la maggior parte delle grandi imprese, il numero di fornitori che forniscono servizi può essere significativo, e in molti casi viene eseguita erroneamente solo una revisione sommaria della maggior parte di essi. Inoltre, in

alcuni casi i fornitori non hanno meccanismi in essere per identificare quando terze parti accedono al loro sistema.

Sempre restando legati ai rischi dei fornitori, una particolare analisi deve essere fatta circa i programmi di gestione delle patch.

Nel caso dei fornitori di software questi giocano un ruolo importante in quanto rilasciano regolarmente aggiornamenti e patch ai loro programmi per poter contrastare le esposizioni al rischio precedentemente identificato.

I maggiori rischi in questo ambito vengono identificati nel momento in cui, una volta emessa la patch dal fornitore, spetta all'entità stessa di testarla, configurarla correttamente sull'infrastruttura IT interessata, e tenuta aggiornata al fine di aiutare a garantire che l'ambiente complessivo rimanga sicuro. È proprio in queste attività di elevata complessità che spesso possono essere commessi errori legati al fattore umano.

4.4.3 Progettazione e implementazione

Se gli attacchi informatici rappresentano un rischio di inesattezze significative nel bilancio, il team di revisione deve progettare procedure appropriate, in coordinamento con i professionisti cyber di supporto, per affrontare il rischio identificato.

Molte funzioni di audit interno eseguono le loro analisi intorno alla valutazione della prontezza di risposta della sicurezza informatica nelle organizzazioni.

Queste analisi mirate però non sempre forniscono garanzie su tutto lo spettro dei rischi di sicurezza informatica; affinché l'audit interno fornisca una visione completa della sicurezza informatica ed eviti di dare una sbagliata sensazione di sicurezza eseguendo solo audit mirati, è necessario impiegare un approccio più ampio.

Oltre alla valutazione del rischio informatico, che costituisce la base dell'analisi fornita al comitato di controllo, è necessario sviluppare mediante i risultati

ottenuti un piano di audit interno pluriennale basato sul rischio per la sicurezza informatica.

Il piano pluriennale può essere sviluppato attraverso i risultati della valutazione dei rischi informatici; in base alle urgenze, alle considerazioni di specifici test e alle attività di valutazione in corso nell'organizzazione, vengono definite le attività di auditing da attuare.

Il piano di audit interno può sicuramente presentare aggiustamenti e adeguamenti in base all'emergere di nuovi rischi, cambiamenti nell'intensità relativa e nell'importanza delle minacce esistenti e di altri sviluppi organizzativi.

Conclusioni

Con questo lavoro di tesi ho voluto enfatizzare l'importanza che ha acquisito il ruolo dell'Auditor IT all'interno di un progetto di revisione contabile per capire quali possano essere gli sviluppi futuri che questa professione adotterà in un'ottica di costante miglioramento del sistema. In un primo momento è stata descritta l'evoluzione della figura dell'auditor, partendo dalla nascita del sistema di controllo, analizzando le varie normative che hanno reso il compito del revisore cruciale ai fini della valutazione finanziaria d'azienda. Nel secondo capitolo il focus si è spostato sull'Audit IT in quanto, in concomitanza con l'introduzione delle strutture IT all'interno delle organizzazioni, è sorta la necessità di implementare una nuova linea di audit che volgesse la sua attenzione sull'affidabilità dei sistemi informativi societari.

È stato quindi analizzato il rischio IT e con esso sono state definite le attività che il team di Audit IT è tenuto a svolgere per supportare il progetto di revisione contabile. La descrizione delle attività svolte dall'auditor IT è stata quindi presentata attraverso l'applicazione di un caso concreto in un ciclo di auditing IT. Tutto ciò grazie allo svolgimento di un progetto di tirocinio curricolare svolto all'interno della società EY, in cui ho avuto modo di apprendere molte informazioni sulla struttura IT delle aziende e le nozioni riguardo la metodologia applicata dalla società di revisione. L'esperienza di lavoro che ho maturato in questo contesto aziendale mi ha permesso di capire l'importanza del ruolo svolto dall'auditor IT, ovvero quello di essere un revisore con conoscenze approfondite in ambito tecnologico, capace di analizzare i nuovi tipi di rischi connessi alle tecnologie digitali che utilizzano i clienti revisionati.

Infine, nell'ultimo capitolo, l'attenzione si è spostata sui cambiamenti che stanno oggi interessando il mondo dell'audit interno. La rapida progressione tecnologica dei sistemi informativi e le minacce correlate rendono necessarie un sistema di sicurezza informatico che deve essere validamente testato e rivisto periodicamente. L'adozione di un piano di audit in ottica cyber security è quindi il modo migliore per determinare la sicurezza delle informazioni di un'organizzazione, senza dover incorrere in costi o altri danni associati a un incidente di sicurezza.

Indice delle Figure:

Indice delle Tabelle: