POLITECNICO DI TORINO

Corso di Laurea Magistrale

Ingegneria Gestionale – percorso Innovazione

Tesi di Laurea Magistrale

Compliance SOX, come cambia la governance ICT

Relatore

Prof. Luigi Buzzacchi

Candidato

Antonio Lucisano

Correlatore

Dott. Federico Volpini

INDICE

ABSTRACT

Il presente lavoro di tesi illustra l'attuale ruolo di un auditor Information Technology (IT), evidenziando le principali cause del radicale cambiamento avvenuto nel corso dell'ultimo ventennio.

Il lavoro è introdotto da una breve lettura storica, indispensabile per inquadrare il sistema capitalistico degli ultimi anni del '900 e sottolineare l'innovazione immessa dalle normative atte a regolamentare il mercato complesso della revisione.

Approfondendo il ruolo della Governance Information and Communication Technology (ICT), lo scopo è legittimare il rinnovamento avvenuto nel corso degli anni, in risposta agli scandali finanziari accaduti a causa dell'inadeguata capacità di gestione. Si analizza quindi l'introduzione del Sarbanes-Oxley Act (SOX) del 2002 in risposta alla mancanza di trasparenza da parte delle grandi società dell'epoca, e come questa normativa abbia influenzato il rinnovamento della Governance.

L'obiettivo del lavoro è validare i meccanismi che hanno portato all'odierna organizzazione aziendale di società americane quotate in borsa.

L'elaborato di tesi nasce dall'esperienza acquisita per merito del tirocinio curriculare, svolto presso la società di revisione contabile Ernst & Young Advisory S.p.A.

Il lavoro è strutturato nelle seguenti sezioni:

- Inquadramento del contesto storico generale.
- Analisi finalizzate ad esplicitare la struttura portante delle società che si occupano di revisione contabile, col fine di chiarire perché attualmente, a questa tipologia di organizzazioni, è assegnata così tanta rilevanza.
- Illustrazione del caso studio, sulla base delle tematiche trattate durante i mesi di esperienza aziendale, in modo da poter sottolineare l'importanza di alcune tipologie di controlli, svolti per garantire maggior sicurezza in ambito IT, e la conseguente mitigazione dei rischi associati.

L’importanza dei dati e delle informazioni da essi ricavate, hanno un ruolo decisivo per la compiutezza dell’intero elaborato di tesi.

- Focus conclusivo per indicare le linee di una prospettiva di sviluppo della tecnologia di interesse, definita sulla base di spunti interpretativi personali.

CAPITOLO I

LA NORMATIVA SOX NEL CONTESTO STORICO ED ECONOMICO DEL 2000

1.1 INTRODUZIONE

Gli anni ’80 e ’90 del ‘900 hanno visto l’America protagonista sui mercati internazionali. Come spesso è accaduto nella storia borsistica, il mercato americano presentava trend rialzisti tali da influenzare investitori di tutto il mondo, in particolare nel settore tecnologico.

Osservando i principali indici azionari nell’arco di tempo compreso tra gli anni ’80 e i primi del 2000, è facile accorgersi di questa impennata. Nella Primavera del 1982 l’indice S&P500[1] quotava 109 punti per arrivare nel 2000 fino ad un massimo di quasi 1.500 punti. Il Nasdaq[2], invece nello stesso periodo, passava da 184 punti, a circa 5.000 (Grafico 1.1). Entrambi gli indici crescevano a dismisura, ma tra i due il Nasdaq era quello con un delta maggiore. La ragione di questo trend va ricercata nella natura stessa dell’indice; infatti, essendo costituito dalle prime 100 società non finanziarie, quasi tutte appartenenti al settore tecnologico, il Nasdaq è fortemente influenzato dalle innovazioni.

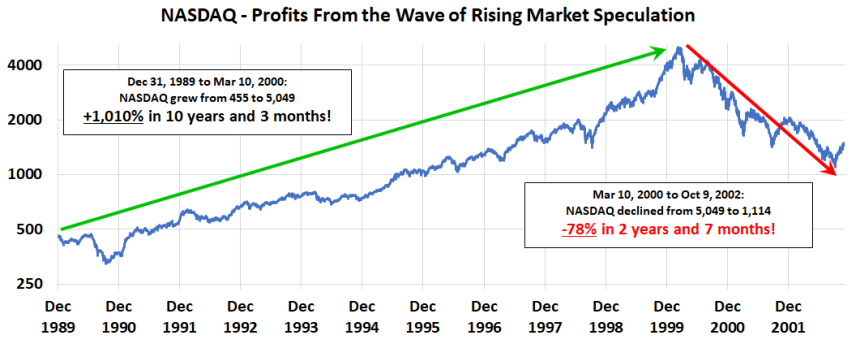


Grafico 1.1: Performance del Nasdaq dal 1990 al 2002. Fonte:Nightingale Advisors

[1] ***S&P 500***: il più importante indice azionario statunitense. È stato creato da Standard & Poor's nel 1957 e segue l'andamento di un paniere azionario formato dalle 500 aziende statunitensi a maggiore capitalizzazione. Rappresenta l’80% circa della capitalizzazione del mercato americano.

[2] ***Nasdaq*** *(“National Association of Securities Dealers Automated Quotation”):* istituito a Wall Street l’8 febbraio 1971 è una delle Borse più influenti al mondo. Primo esempio di mercato borsistico elettronico.

Il valore di azioni sconosciute impennava senza preavvisi, passando da pochi centesimi di dollaro a diverse centinaia, in pochissimo tempo. Alla fine degli anni ’90, gli investitori che riuscirono a capitalizzare miliardi erano molteplici. La maggior parte delle aziende, in realtà, non produceva nulla, eppure, capitalizzava più di General Motors, Ford ed altri colossi dell’industria mondiale di allora.

Erano gli anni dell’avvento di internet e la prima cosa che influenzava direttamente i mercati, era l’introduzione del trading online. Era sufficiente che un’azienda annunciasse un progetto relativo ad internet, che aprisse un sito, o che intraprendesse una qualunque innovazione inerente al virtuale, affinché registrasse enormi rialzi in Borsa. I grafici e le informazioni economiche iniziavano ad essere a disposizione di chiunque; le attività borsistiche, fino a pochi anni prima riservate esclusivamente agli addetti ai lavori, venivano concesse anche ai non professionisti. Non era più necessario conoscere, telefonare, acquisire informazioni, da un capo all’altro del mondo, era sufficiente un click.

Era questo il contesto in cui si presentava l’America all’alba del nuovo millennio; un ambiente florido, euforico e pronto ad abbracciare una realtà “più virtuale”.

Tuttavia, come è già rappresentato nel Grafico 1.1, l’inizio del nuovo millennio vide per il Nasdaq, una caduta vertiginosa dei profitti relativi. L’America stava andando incontro a una delle più colossali crisi dell’era moderna.

1.2 IL 2001 E IL CASO ENRON

La Enron nacque nel 1985 con Kenneth Lay, dalla fusione della Houston Natural Gas con l'Iner North del Nebraska. Con il passare del tempo, l'espansione della multinazionale fu tale da estendersi in tutto il Nord America ed in Gran Bretagna. L'azienda iniziò la diversificazione del proprio business attraverso strategie basate su investimenti in carbone, acciaio, acqua e internet. Era un'azione totalmente nuova e radicale per un'azienda di quel periodo, ci si muoveva verso una New Economy fatta di territori virtuali. Questa condizione fu accolta piacevolmente da numerosi analisti economici; l'Economist definì la Enron addirittura un "culto evangelico". Dagli anni '90 in poi lo sviluppo divenne ancora più frenetico; con la guida di Jeffrey Skilling, la compagnia arrivò ad essere la più importante protagonista del commercio libero dell'energia elettrica. I miliardi di dollari spesi in energia elettrica, movimentati giornalmente dalla società, ebbero però l'effetto di aumentare i costi di produzione della stessa, facendo indebitare interi stati, come per esempio, la California.

"Il modello Enron fu ben descritto da uno dei tanti ex-dipendenti danneggiati: «I boss si limitavano a prendere il denaro fuori dal palazzo per portarlo dentro. Solo che Skilling ha fatto una cosa ancora più intelligente: ha lasciato il palazzo, e si è portato dietro i soldi». Perfino quando il boom dei nuovi mercati e delle transazioni fece salire il valore dei dividendi, e quindi anche i bonus per i dirigenti, la compagnia continuò a fare uscire più soldi di quanto ne entravano. Così i contabili della Enron cominciarono a usare trucchetti complicati per far sparire miliardi di dollari di debiti dai propri bilanci, inventando alleanze e partnership che non esistevano per mantenere la finzione della prosperità".[3]

[3] Articolo dell'associazione politico culturale Marx21 del 27 Maggio 2006.

Enron era inoltre complice di rapporti tutt'altro che legali con la Arthur Andersen, colosso nell'ambito della revisione contabile, che si occupava della verifica della 'correttezza' dei bilanci della multinazionale texana. A metà del 2001 Skilling e Lay abbandonarono la società, lasciando ammanchi notevoli che si sarebbero rivelati incolmabili.

Ad ottobre del 2001 la situazione era tragica, il capitale degli azionisti era diminuito di 1,2 miliardi di dollari nel terzo quadrimestre. Fu aperta un'inchiesta formale. La prima reazione degli investitori, insospettiti dal fatto che la Enron poteva nascondere forti perdite, fu di vendere. Il valore delle azioni a dicembre del 200 scese a 36 centesimi, rispetto ai 90 dollari dell'anno precedente (Grafico 1.2)[4].

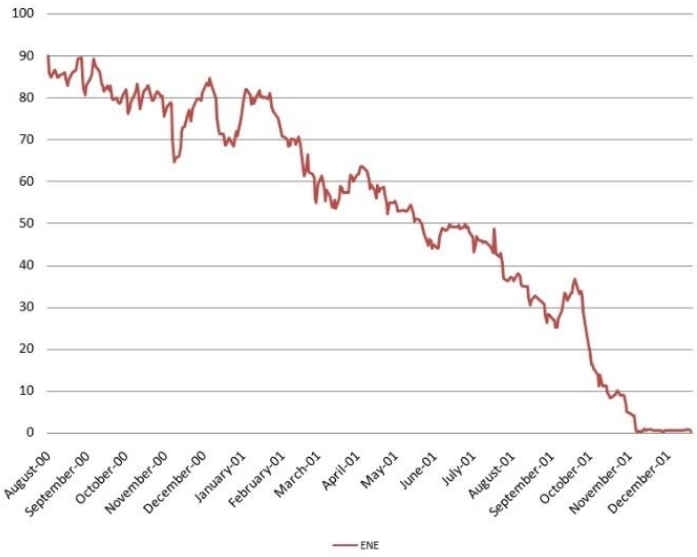


Grafico 1.2:Enron stock price from August 23, 2000 to January 11, 2002. Fonte: Course Hero, Business Ethics

[4] Sull'asse delle ordinate è indicato il prezzo delle azioni in dollari.

Il 2 dicembre del 2001 la Enron dichiarò fallimento. Da tempo sotto lo stretto controllo della Sec (Consob americana), la società fu dichiarata colpevole di frode e cospirazione. Dal momento del crollo tutte le azioni dei creditori vennero bloccate, i contratti congelati e la società, dichiarata in dissesto finanziario, passò sotto la giurisdizione della corte federale. Di seguito si riportano due articoli tra i più significativi, al fine di inquadrare il pensiero generato dagli scandali del periodo in considerazione:

"Le sorti di Enron, il colosso mondiale dell'energia, sono appese a un filo. Il gruppo di Houston, Texas, ha infatti annunciato l'immediato stop a tutti i pagamenti e potrebbe essere costretto a cercare protezione dai creditori ricorrendo al Capitolo 11 del Bankruptcy Code. Sarebbe il più grande fallimento della storia industriale americana. [...] I tempi in cui il gruppo guidato da Kenneth Lay e Jeff Skilling veniva definito dalla rivista Fortune come "il più innovativo d'America" sembrano ormai lontanissimi".[5]

"C'è stato un fallimento totale da parte di tutti, un completo guasto nel sistema, in tutti i controlli e gli equilibri. È stato un fallimento da parte degli analisti di Wall Street che sono appena andati avanti per la corsa, e dai revisori che stavano raccogliendo così tanti soldi che non potevano andarsene, e dalle agenzie governative che dovrebbero monitorare quelle società".[6]

Il fallimento della Enron è stato il primo di una serie. Un altro caso tra i più eclatanti è rappresentato dalla WorldCom, mega-corporation con un valore di mercato tre volte più grande rispetto alla Enron nel periodo antecedente allo scoppio della bolla speculativa. Si riporta di seguito il Grafico 1.3, atto a quantificare le perdite finanziarie più rilevanti dell'ultimo ventennio. Dalla lettura del Grafico 1.3 si constata che la Enron e la Worldcom, sono seconde solo ad aziende che hanno dovuto fare i conti con l'ulteriore crisi finanziaria del 2007.

[5] Tratto da un articolo del Corriere della Sera del 3 Dicembre 2016.

[6] Tratto da un articolo del Los Angeles Times del 26 gennaio 2002, meno di due mesi dopo che Enron aveva presentato istanza di fallimento

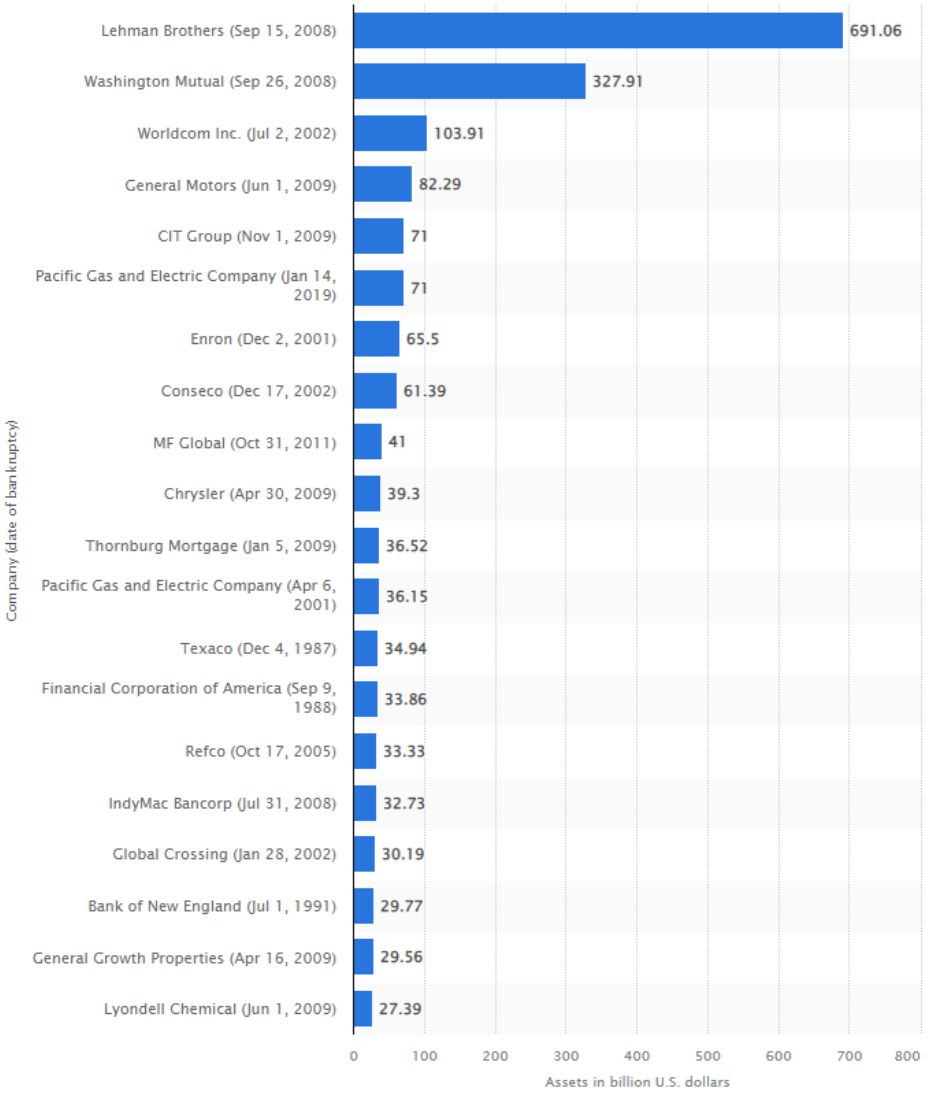


Grafico 1.3: Le più gravi bancarotte dal 2000 a oggi. Fonte: Statista

1.2.1 LA SPIEGAZIONE DEL CRACK TRA LE PIEGHE DEI BILANCI SOCIETARI

Dietro i numeri altisonanti del fatturato e le certificazioni dei bilanci da parte delle società di revisione cui si appoggiava la Enron, si nascondevano in realtà cifre fasulle. Attraverso stratagemmi contabili, in grado di eludere i controlli, e potendo contare su conoscenze e coperture politiche, i numeri venivano ritoccati ad arte.

Un'abilità della super-corporation texana fu anche quella di trovare metodi per gonfiare i propri profitti, distribuendo i ricavi all'interno di una fitta rete di società situate in paradisi fiscali come le Isole Cayman, usufruendo di notevoli agevolazioni sulle tassazioni. Il valore delle azioni, se pur falsato, rimaneva in questo modo stabile.

Di seguito si riporta uno stralcio dell'articolo del Corriere della Sera di gennaio 2002, in cui fu descritto il rapporto della Enron con la Andersen, e i meccanismi con cui si innescò il processo che provocò la caduta di società terze, estranee ai fatti, come fossero tessere di domino.

"Un complesso gioco di scatole cinesi, avallato da chi, in teoria, avrebbe dovuto «controllare» i bilanci e che invece partecipava alla truffa. «La Enron ha derubato la banca», disse 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». Nei procedimenti giudiziari successivi furono coinvolti i vertici di Andersen, in particolare la responsabile legal Nancy Temple e il referente per Enron David Duncan, provocando il blocco operativo della società — oltre alla perdita dei maggiori clienti — nonostante il nulla di fatto deciso nel 2005 dalla Corte Suprema, per un vizio di forma nelle istruzioni date alla giuria del primo processo. Decisione, questa, che non salvò comunque il colosso Andersen, costretto dopo poco a chiudere, come peraltro molte società coinvolte direttamente con Enron, o peggio, vittime della spirale provocata dal crac della multinazionale texana. Emblematico in proposito fu il caso della catena di supermercati Kmart, costretta al fallimento dopo che molte banche americane, indebitate con Enron, richiesero un rientro dei

crediti ai loro debitori. La stessa sorte toccò ad alcune società assicurative incaricate dei risarcimenti".[7]

In conclusione, la Enron descritta come una società impegnata nel settore degli idrocarburi, si trasformò progressivamente, in un intermediario fra produttori e consumatori di energia. Truccando i bilanci, evadendo le tasse e potendo contare su un forte appoggio politico, applicò formule di ingegneria finanziaria sperimentate all'interno del mercato, e riuscì a trarre un enorme vantaggio economico, se pur temporaneo, basando la sua credibilità su numeri in realtà vuoti e privi di significato.

L'America nei primi anni del 2000 visse un tragico periodo, caratterizzato dal susseguirsi di disastrosi crolli per cui gli organi legislativi furono chiamati a rispondere.

[7] Articolo del corriere della Sera del 19 gennaio 2002

1.3 NASCITA DELLA SOX E DEL PCAOB

Come sottolineato in precedenza sono stati molti i default finanziari nell'ultimo ventennio, ma se da un lato Enron non rappresenta il caso più grave, dall'altro è stato sicuramente il simbolo della spregiudicatezza finanziaria, che segnò il punto di svolta nell'economia americana. Il mondo della finanza dopo il 2001, si apprestò ad abbracciare grandi cambiamenti, soprattutto sotto il punto di vista dei controlli. Grazie a una reazione immediata dell'opinione pubblica contro gli scandali di Wall Street nacque una nuova giurisprudenza antitrust: nel luglio del 2002 fu istituita la legge Sarbanes-Oxley.

«Tra dieci anni, non le stragi dell'11 settembre, ma lo scandalo Enron sarà visto come la grande svolta degli Stati Uniti». Così si espresse il professor Paul Krugman, premio Nobel per l'economia nel 2008, un anno dopo il fallimento Enron, con la speranza che l'esempio della società texana potesse indurre ad un cambiamento radicale del mondo finanziario. Ad oggi, il mercato azionario americano segue ancora la legge emanata in conseguenza di quel disastro: Krugman aveva avuto ragione.

In un contesto in cui la speculazione era crescente e la fiducia dei risparmiatori vacillava sempre di più, un cambio di passo era necessario. Questa svolta fu possibile grazie al Sarbanes-Oxley Act. La legge fu una vera e propria rivoluzione, tanto radicale, quanto opportuna, anche se entrare rapidamente e bene, all'interno di un'organizzazione finanziaria totalmente rinnovata, fu indubbiamente difficile.

Il collasso della Enron e delle società ad essa legate, forse furono eventi meno rumorosi rispetto alla tragedia dell'attentato dell'11 settembre del 2001 alle Torri Gemelle, ma provocò perdite altrettanto gravi per l'America e gli americani. Non a caso questo tracollo fu definito 'l'11 settembre del liberismo e del capitalismo'. Nuovi provvedimenti rigidi e irreversibili furono necessari.

Per notare il radicale cambiamento, basti pensare che precedentemente a questi fatti, si effettuavano controlli semplici, di routine; successivamente invece, si dovettero applicare norme restrittive e di controllo severo, sia nell'ambito dei trasporti che in quello finanziario.

La legge SOX fissò le nuove regole nel settore finanziario di interesse.

Il Sarbanes-Oxley Act fu approvato dal Senato e dalla Camera dei rappresentanti degli Stati Uniti nel luglio del 2002 (Pub. L. 107-204, 116 Stat. 745, 30 luglio 2002). La legge, adesso conosciuta anche con il nome di "Public Company Accounting Reform and Investor Protection Act of 2002" è comunemente chiamata Sarbox o SOX. Essa ebbe origine da due proposte di legge presentate rispettivamente dal deputato Mike Oxley e dal senatore Paul Sarbanes. Successivamente, i testi furono unificati ed approvati a maggioranza da una commissione bicamerale in un unico atto finale, firmato da George W. Bush il 30 luglio.

La Sarbox non fu solamente una necessaria risposta alla Enron, nonostante i disastri che il suo fallimento provocò, ma ebbe origine affinché i dati potessero diventare trasparenti a tutela degli investitori. Le regole sulla divulgazione e sul reporting furono totalmente riscritte.

L'obiettivo principale fu quello di chiudere alcune "falle" all'interno della legislazione americana, al fine di migliorare la 'Corporate Governance'[8] delle aziende e garantire la trasparenza delle scritture contabili. Anche l'aspetto penale fu inasprito con l'incremento delle pene per i casi di falso in bilancio e simili, con conseguente aumento della responsabilità dell'auditor, nell'atto di revisione contabile.

[8] ***Corporate Governance:*** insieme degli strumenti, delle regole, leggi, relazioni, e in generale di tutti i processi finalizzati a una corretta gestione di un'impresa.

La normativa SOX, tutt'ora vigente, ha introdotto nuove procedure per le verifiche contabili, stabilendo che tutte le aziende pubbliche aventi titoli in borsa americana, devono soddisfare i requisiti espressi dalla legge.

"Sotto la miriade di pagine dell'atto di legalese, si trova una semplice premessa: il buon governo societario e le pratiche commerciali etiche non sono più sottigliezze: sono la legge. Dietro tutte le regole, requisiti, certificazioni ed attestazioni, il Sarbanes-Oxley Act è il modo con cui dispone l'intervento giuridico nei precetti di base della buona governance aziendale e delle pratiche commerciali etiche. Sarbanes-Oxley codifica il punto di vista secondo cui il management aziendale deve conoscere le informazioni ed i materiali depositati presso la SEC[9] e rilasciate agli investitori, e diventa così responsabile della correttezza, completezza e accuratezza di tali informazioni".[10]

Contemporaneamente al Sarbanes-Oxley Act fu istituito anche il "Public Accounting Oversight Board" (PCAOB) il consiglio di vigilanza sui bilanci delle aziende quotate; un'organizzazione senza scopo di lucro che regola i revisori dei conti di società quotate in borsa. Il PCAOB protegge gli investitori e gli altri stakeholder delle società pubbliche, assicurando che i revisori seguano linee guida rigorose. Se la SOX può essere vista come una risposta al caso Enron, il PCAOB lo è, a pari modo, nei confronti delle società come la Andersen.

Controllato dalla Securities and Exchange Commission dal 2010, il consiglio supervisiona gli audit di broker e dealer registrati alla SEC. Le società che controllano società pubbliche, broker e rivenditori sono obbligati a registrarsi al PCAOB e sono soggette all'ispezione degli audit da loro svolti. Il PCAOB inoltre è coinvolto nella definizione di standard volti a migliorare l'affidabilità degli audit e può anche far rispettare gli standard imponendo sanzioni per le infrazioni. Governato da cinque membri designati per cinque anni i termini dalla SEC in coordinamento con il consiglio dei governatori della Federal Reserve System e il Segretario del Tesoro. La missione principale Public Company Accounting

[9] ***SEC*** *(Securities and Exchange Commission*): è l'ente federale statunitense preposto alla vigilanza della borsa valori.

[10] Guida di Deloitte&Touche del gennaio 2003: Moving Forward-A Guide to Improving Corporate Governance Through Effective Internal Control

Oversight Board è quella di analizzare il rapporto tra le imprese di contabilità pubblica e dei loro clienti. Una sorta di sorvegliante primario della legislazione SOX e di come le aziende implementano i principi contabili richiesti nelle loro pratiche commerciali.

STRUTTURA DEL PCAOB:

l'atto stabilisce che il PCAOB ha sede in Washington DC ed è un organismo senza scopo di lucro.

- È composto da cinque membri;
- Ciascun membro è scelto dalla SEC;
- Ciascun membro ricopre l'incarico per cinque anni;
- La posizione è a tempo pieno;
- Due membri devono essere CPA[11];
- È finanziato dalle società quotate;
- Le spese di registrazione sono pagate dalle società di revisione.

La SEC deve approvare, riguardo al PCAOB, il budget annuale e le regolamentazioni proposte, includendo gli standard di revisione.

Lo scopo del PCAOB è quello ridurre al minimo il rischio di audit. Ma perché è così importante ridurre questo rischio, tanto da costituire un organo giuridico?

Il rischio di audit o di revisione è il rischio che il bilancio sia sostanzialmente errato, anche se il giudizio di revisione afferma che i rendiconti finanziari sono privi di errori significativi. Questa eventuale svista potrebbe condannare qualunque azienda. Il motivo per cui viene impegnata una considerevole quantità di risorse è cercare di mitigare questo rischio. Se fosse riducibile allo 0% non si potrebbe parlare di rischio, ma i numerosi controlli crescenti, iniziati a seguito delle normative del 2001, garantiscono maggiore sicurezza nel

[11] ***CPA***: Certified Public Accountants - contabile pubblico certificato

trattamento dei dati. Lo scopo di un audit è quindi quello di ridurre il rischio di revisione a un livello basso, attraverso test e prove sufficienti. Poiché i creditori, gli investitori e altre parti interessate fanno affidamento sul bilancio, il rischio di revisione può comportare la responsabilità legale per una società di CPA che esegue attività di revisione. Le due componenti del rischio di revisione sono il rischio di errori significativi e il rischio di individuazione. Di seguito si riporta un esempio delle due diverse tipologie di rischio:

"Si supponga che un grande negozio di articoli sportivi necessiti di una verifica e che un'azienda stia valutando il rischio di controllare l'inventario del negozio.

1. Il rischio di errori significativi è il rischio che i rendiconti finanziari siano sostanzialmente errati prima che venga eseguita la revisione contabile. un importo o una percentuale in dollari sufficientemente grande da modificare l'opinione di un lettore di rendiconti finanziari rappresenta il rischio ed è soggettivo. Se il saldo dell'inventario del negozio di articoli sportivi di $ 1 milione non è corretto di $ 100.000, uno stakeholder che legge il rendiconto finanziario può considerarlo un importo significativo. Il rischio di errori significativi è ancora maggiore se si ritiene che i controlli interni siano insufficienti, che è anche un rischio di frode.

2. Il rischio di individuazione è il rischio che le procedure del revisore non rilevino un errore significativo. Ad esempio, un revisore deve eseguire un conteggio fisico dell'inventario e confrontare i risultati con le registrazioni contabili. Questo lavoro viene eseguito per dimostrare l'esistenza stessa dell'inventario. Se il campione di prova del revisore per il conteggio dell'inventario non è sufficiente per estrapolare l'intero inventario, il rischio di individuazione è maggiore".[12]

[12] KamilTaylan.blog, enciclopedia finanziaria

1.4 ANALISI DELLE PRINCIPALI SEZIONI DELLA NORMATIVA SOX

Le disposizioni della legge Sarbanes-Oxley sono suddivise in sezioni numerate. Di seguito si riportano i titoli che compongono la struttura del Sarbanes-Oxley Act e le sezioni di maggior interesse per la sicurezza informatica.

STRUTTURA DEL SARBANES-OXLEY ACT:

Title I – Public Company Accounting Oversight Board

Title II – Auditor Independent

Title III – Corporate Responsability

Title IV – Enhanced Financial Disclorusw

Title V – Analyst Conflict of Interest

Title VI – Commission Resources and Authority

Title VII – Studies and Reports

Title VIII – Corporate and Criminal Fraud Accountability

Title IX – White-Collar Crime Penalty Enhancement

Title X – Corporate Tax Returns

Title XI – Corporate Fraud and Accountability

Sezione 302: Corporate Responsability for Financial Reports

“Ai sensi della Sezione 302, i CEO e i CFO devono certificare personalmente di essere responsabili dei controlli e delle procedure di divulgazione. Ogni fascicolo trimestrale deve contenere una certificazione che attesti che sia stata effettuata una valutazione della progettazione e dell'efficacia di tali controlli. I responsabili della certificazione devono inoltre 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".[13]

La sezione 302 rappresenta forse la parte più importante di tutto l'atto legislativo e conferisce maggiore responsabilità per i CEO e per i CFO, che assumono l'obbligo di certificare in prima persona che i controlli e le procedure di divulgazione vengano implementati e valutati. Pone, inoltre, l'accento sui ruoli delle figure di cui sopra, in particolare, per ogni presentazione trimestrale e annuale sia CEO che CFO hanno l'obbligo di:

- Essere responsabili dei controlli e delle procedure di comunicazione effettuate;
- Progettare, o supervisionare, la progettazione dei controlli al fine di assicurare che le informazioni rilevanti siano rese note;
- Valutare l'efficacia dei controlli;
- Presentare le conclusioni in merito all'efficacia dei controlli;
- Comunicare 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 significativo nel controllo interno della società;
- Indicare nel deposito eventuali modifiche significative.

Sezione 401: Disclosures in Periodic Reports

"La Sezione 401 specifica che le informazioni finanziarie fornite al pubblico in qualsiasi rapporto fornito alla SEC non conterranno dichiarazioni non veritiere o omissioni di fatti materiali e saranno conformi ai principi contabili generalmente accettati (GAAP). I report includeranno tutte le transazioni fuori bilancio rilevanti".[14]

[13] Section 302: Corporate Responsibility for Financial Reports - SoxLaw
[14] Section 401: Disclosures in Periodic Reports - SoxLaw

Sezione 404: Management Assessment of Internal Controls

"La sezione 404 prevede una valutazione annuale dei controlli interni e delle procedure per l'informativa finanziaria. Inoltre, il revisore indipendente della società di revisione deve redigere una relazione separata che attesti l'affermazione del management sull'efficacia dei controlli interni e delle procedure per l'informativa finanziaria". [15]

Come la Sezione 302, anche la Sezione 404, richiede che i CEO e i CFO valutino periodicamente e garantiscano l'efficacia di questi controlli. Le società vengono quindi obbligate a redigere all'interno della rendicontazione annuale un 'rapporto di controllo interno del management' che:

- Affermi di essere stati responsabili dell'istituzione e del mantenimento dei controlli interni e delle procedure di informativa finanziaria;
- Valuti e giunga a conclusioni sull'efficacia dei controlli interni e sulle procedure di informativa finanziaria;
- Dichiari che la società di revisione contabile abbia attestato e riferito in merito alla valutazione, da parte del management, dei controlli interni e delle procedure di informativa finanziaria della società.

In base alle norme SEC proposte, i dirigenti hanno il compito di certificare, con una frequenza trimestrale, l'effettiva efficacia dei loro controlli interni e delle procedure di rendicontazione finanziaria. Inoltre, viene richiesta al revisore indipendente di una società di revisione contabile di compilare una relazione separata che attesti la valutazione del management sull'efficacia dei controlli interni e delle procedure per l'informativa finanziaria.

Nei primi periodi successivi all'emanazione dell'atto, sono stati stabiliti nuovi processi per eseguire la valutazione della conformità e il monitoraggio.

"Esempi di processi creati o rafforzati possono essere:

- Processi che consentono ai dipendenti di segnalare potenziali debolezze nel controllo e di determinare le azioni appropriate da intraprendere;

[15] Section 404: Management Assessment of Internal Controls - SoxLaw

- Processi per la gestione delle questioni relative all'informativa;
- Processi per la valutazione degli impatti e delle implicazioni di compliance di cambiamenti significativi del business (ad esempio, fusioni, acquisizioni, nuove relazioni di outsourcing, cambiamenti nella struttura organizzativa);
- Processi per l'individuazione e la qualificazione dei dipendenti cui è stata attribuita la responsabilità delle valutazioni del controllo interno;"[16]

Sezione 409: Real Time Issuer Disclosures

"La sezione 409 di SOX afferma: "Gli emittenti sono tenuti a divulgare al pubblico, su base urgente, informazioni su cambiamenti sostanziali nelle loro condizioni finanziarie o operazioni. Queste informazioni devono essere presentate in termini che siano di facile comprensione e supportati da informazioni di tendenza e qualitative delle presentazioni grafiche, a seconda dei casi."[17]

Questa interessante sezione costringe le aziende a divulgare cose che potrebbero preferire non pubblicizzare, come una violazione dei dati o altri attacchi informatici che hanno un impatto sulle operazioni.

Sezione 802: Criminal Penalties for Altering Documents

"La sezione 802 del Sarbanes Oxley Act impone pene fino a 20 anni di reclusione per l'alterazione, la distruzione, la mutilazione, l'occultamento, la falsificazione di registri, documenti o oggetti tangibili con l'intento di ostacolare, impedire o influenzare un'indagine legale. Un contabile o un revisore contabile che viola consapevolmente e intenzionalmente l'obbligo di conservare i registri per cinque anni può anche essere soggetto a un massimo di dieci anni di carcere."[18]

[16] Guida di Deloitte&Touche del gennaio 2003: Moving Forward-A Guide to Improving Corporate Governance Through Effective Internal Control
[17] Section 409: Real Time Issuer Disclosures - SoxLaw
[18] Section 802: Criminal Penalties for Altering Documents - SoxLaw

Sezione 806: Protection for Employees of Publicly Traded Companies Who Provide Evidence of Fraud

In risposta agli avvenimenti del caso Worldcom nasce questa sezione conosciuta come 'Protection for Whistleblowers'. A scopo tutelativo, nei confronti degli informatori, la legge delega il Dipartimento del Lavoro per proteggere gli informatori dalle ritorsioni dei datori di lavoro, autorizzando, inoltre, il Dipartimento di Giustizia a sporgere denuncia penale contro i responsabili delle ritorsioni.

Al dipendente viene riconosciuta la protezione nel momento in cui segnala la presenza di:

- "frode federale di posta, bonifico, banca o titoli;
- una violazione della legge federale relativa alla frode contro gli azionisti;
- una violazione di qualsiasi norma o regolamento della Securities and Exchange Commission (SEC)."[19]

Sezione 902: Attempts & Conspiracies to Commit Fraud Offenses

"La Sezione 902 fa parte del titolo 'White Collar Crime Penalty Enhancement'. Secondo questa sezione chiunque tenti o cospiri per commettere qualsiasi reato ai sensi del presente capitolo sarà soggetto alle stesse pene prescritte per il reato, le cui commissioni sono state oggetto del tentativo o della cospirazione. Il che significa che un dirigente che viola la SOX in modo fraudolento sarà soggetto alle solite sanzioni, che si tratti di multe o carcere, per frode."[20]

[19] Section 806: Protection for Employees of Publicly Traded Companies Who Provide Evidence of Fraud - SoxLaw

[20] Section 902: Attempts & Conspiracies to Commit Fraud Offenses - SoxLaw

Sezione 906: Corporate Responsibility for Financial Reports

"Questa sezione richiede ai CEO e ai CFO di firmare e certificare la relazione periodica contenente i rendiconti finanziari; la certificazione esecutiva afferma che la relazione è conforme ai requisiti di reporting della SEC e rappresenta correttamente la condizione finanziaria dell'azienda e i risultati delle sue operazioni; il mancato rispetto di questo requisito comporta un prezzo elevato: multe fino a 5 milioni di dollari e la reclusione fino a 20 anni può essere imposta per non conformità consapevole o intenzionale."[21]

[21] Section 906: Corporate Responsibility for Financial Reports - SoxLaw

1.5 L'IMPORTANZA DELLA TUTELA DEGLI INVESTITORI

«Nei mercati finanziari la fiducia è tutto, e oggi vacilla. I risparmiatori sono preoccupati che in Borsa vi siano altri casi Enron» scrisse nel 2002 Francesco Giavazzi. «La lezione è che la regolamentazione dei mercati è questione troppo seria per essere lasciata in balia di qualche lobby, o preda della gelosia di istituzioni impegnate a giustificare la propria esistenza»

Un dato speciale sottolinea uno dei principi che questo lavoro di tesi enfatizza: l'importanza degli investitori. Il Grafico 1.4 indica il numero di Initial Public Offering (IPO[22]) emesse negli Stati Uniti dal 1999 ad oggi. Se nel 1999 il mercato americano poteva contare su 486 IPO, nel 2001 l'attività si aggirava invece intorno alle 100, uno dei punti più bassi che l'economia americana abbia mai toccato. Se da un lato è vero che gli attacchi terroristici dell'11 settembre 2001 ridussero la liquidità nei mercati e l'attività economica generale, dall'altro è anche vero che le frodi finanziarie dello stesso periodo non giovarono alla borsa americana, contribuendo ad una significativa diminuzione delle offerte pubbliche.

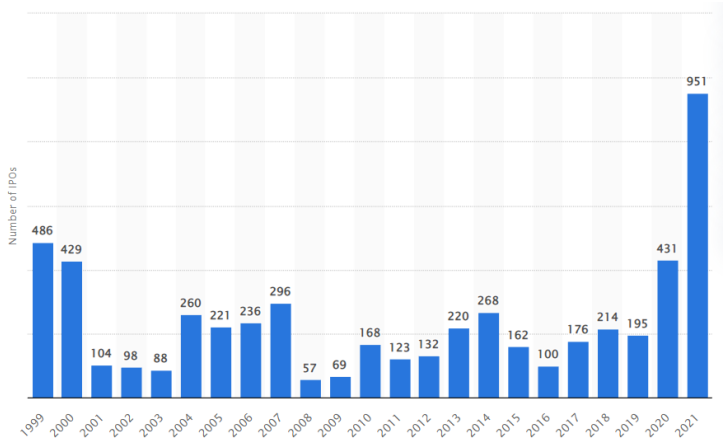


Grafico 1.4: Tratto da Number of IPOs in the U.S. 1999-2022 | Statista.

[22] ***IPO*** *(Initial Public Offering)*: Offerta pubblica iniziale di titoli azionari con cui una società colloca parte di tali titoli per la prima volta sul mercato borsistico, offrendoli al pubblico degli investitori. I dati trattati valutano una IPO come una società operativa sul NYSE, sul Nasdaq o sull'AMEX. Questa definizione esclude ADR, fondi chiusi e azioni scambiate per meno di $ 5

L’inizio del XXI secolo fu considerato dagli analisti un periodo caratterizzato da un’abbondanza di trasgressioni economico-finanziarie. I mercati dei capitali subirono una stangata. Si elencano di seguito le principali cause:

- dot-com bust
- retribuzione eccessiva degli amministratori delegati
- insider trading
- scandali contabili
- riaffermazioni finanziarie
- malversazione dei dirigenti
- frodi
- fallimenti aziendali
- crisi dei fondi comuni d'investimento.

Questa serie di eventi danneggiò gravemente la fiducia degli investitori soprattutto per la qualità delle informazioni storiche e predittive, fornite dalle società pubbliche. E, così come crollò la fiducia, crollò anche la capitalizzazione di mercato di molte tra le società coinvolte.

Il periodo di transizione, successivo alla crisi finanziaria, fu caratterizzato da molta confusione e incertezza. La Sarbanes Oxley mirava a scoraggiare tali reclami per mezzo di alcune misure che rafforzarono i controlli e gli equilibri interni, concentrandosi sul ruolo critico del "controllo interno" ed aumentando al contempo la responsabilità.

Il Sarbanes-Oxley Act intervenne con rilevanti modifiche su alcuni aspetti della disciplina finanziaria, schierandosi a tutela degli investitori, con lo scopo di conferire certezza ed affidabilità riguardo l'informativa di mercato sull'andamento delle società.

Con l'approvazione della legge, delle regole e degli standard associati, si istituirono significativi miglioramenti nel governo societario: i consigli di amministrazione diventarono sempre più indipendenti; i comitati di revisione contabile agirono con ritrovato scetticismo e autonomia; gli amministratori delegati iniziarono ad assumere maggiore responsabilità nella rendicontazione finanziaria.

Tuttavia, ciò non significò che i giorni del fallimento e della frode furono definitivamente relegati al passato. Infatti, nonostante gli apprezzabili progressi compiuti, continuarono a verificarsi nuovi scandali commerciali. La nuova enfasi posta sul governo societario e sul controllo interno avrebbe attenuato le condizioni che contribuivano alla crisi. La Corporate Governance stava diventando fondamentale.

Alla luce dell'intensa copertura mediatica e del controllo normativo, i primi ad adottare forti misure di corporate governance aziendale avrebbero raccolto benefici significativi. Questa teoria era confermata da numerose indagini. Una ricerca condotta da McKinsey & Co. affermava che:

- Il 57% degli investitori istituzionali dichiararono che una buona corporate avrebbe determinato l'aumento o la diminuzione delle partecipazioni in un'azienda;

- Gli investitori erano disposti a pagare un premio per il buon governo, fino al 41%, a seconda del paese di origine;

- Passando dal peggiore al migliore corporate governance, le aziende potevano aspettarsi un guadagno del 10-12 per cento nella loro valutazione di mercato. Un dato insignificante per singola azione, ma che significa un aumento di oltre 1 miliardo di dollari per una società con una capitalizzazione di mercato di 10 miliardi di dollari.

Gli indizi per presagire che la nuova regolamentazione avrebbe garantito rendimenti a lungo termine c'erano tutti.

Non era comunque semplice uniformarsi a una legge tanto complicata. Il prezzo che ogni azienda avrebbe dovuto pagare era quello relativo all'acquisizione di competenze e conoscenze: occorreva far fronte a una riorganizzazione totale del proprio governo societario. Una volta che la corporate governance veniva strutturata correttamente, le società potevano lavorare senza intoppi grazie all'esistenza di un chiaro livello di responsabilità e comunicazione all'interno dell'organizzazione. Per comprendere e utilizzare correttamente la corporate governance era importante comprendere e seguire i cosiddetti 'principi fondamentali'. I principi di tutte le forme di governo societario sono generalmente

legati agli azionisti, ai membri del consiglio di amministrazione e agli stakeholder. La Corporate Governance iniziava inoltre a porre forte enfasi sul comportamento della società e su quanto rivelava al pubblico. Uno dei principi fondanti su cui si doveva basare era proprio la trasparenza, un aspetto molto a cuore anche alla SOX.

La trasparenza si basa sull'idea che la società deve sempre far sapere quali sono le responsabilità e i doveri di coloro che lavorano per la società ed il management, al fine di mantenere una certa responsabilità tra le parti interessate. Un altro aspetto della trasparenza è la divulgazione di materiale relativo alla società che deve essere distribuito in modo da permettere a chiunque abbia investito nella società, di avere un chiaro accesso alle informazioni.

1.6 IL CONTROLLO INTERNO

Analizzando più nel dettaglio ciò che è stato discusso nei paragrafi precedenti, un ruolo fondamentale all'interno del Sarbanes Oxley Act è indubbiamente quello del controllo interno. Gli anni successivi agli scandali del 2001 sono stati quelli in cui i dati e le informazioni assunsero per la prima volta grande importanza. Ad oggi il valore stesso di un'azienda è rappresentato dai dati. La Data Governance[23] ha assunto un ruolo sempre più di primo piano nei contesti aziendali. Se da un lato è vero che le informazioni si contraddistinguono dai dati, dall'altro i dati concorrono in maniera determinante a formarla. Proprio a causa di questo concatenarsi di concetti, occorre stare molto attenti in quanto, se i dati sono univoci, le informazioni da essi estraibili no: dipendono dal significato che l'utente ne vuole attribuire. Un po' come insegna il 'Chinese Whispers' famigerato gioco per bambini, anche conosciuto come telefono senza fili, un'informazione può subire delle alterazioni diventando incomprensibile, talvolta fuorviante, per il diretto interessato. Garantire trasparenza e protezione dei dati da eventuali manipolazioni, rappresenta il fine ultimo che si pone la SOX affinché ogni interlocutore possa operare partendo da materiale oggettivo. Ma come sarebbe stato possibile riuscire in un periodo in cui la parola 'audit' non aveva lo stesso significato di adesso?

Alla data dell'entrata in vigore della Sarbox, le organizzazioni che non disponevano di un'infrastruttura solida e di un ampio staff, dovettero adattarsi ad una conformità particolarmente onerosa. Le aziende di qualsiasi dimensione furono costrette a dedicare risorse significative all'impiego di tempo, denaro e personale. I costi di conformità, sia in dollari che in anni, furono considerevoli (ma non tanto quanto i costi di non conformità). I costi diretti includevano, e in parte includono tutt'ora: il tempo dei dipendenti e dei consulenti per la valutazione; l'implementazione e il monitoraggio; la formazione dei dipendenti sul controllo interno; le spese per le nuove tecnologie a supporto del programma di controllo interno; gli onorari per l'esecuzione di test di controllo da parte dell'auditor indipendente per attestare l'efficacia del controllo interno. I costi indiretti erano composti invece,

[23] ***Data Governance:*** concetto di gestione dei dati relativo alla capacità che consente a un'organizzazione di garantire che esista un'elevata qualità dei dati durante l'intero ciclo di vita dei dati e che vengano implementati controlli su di essi che supportino gli obiettivi aziendali.

principalmente, dalla riassegnazione delle persone e dal riallineamento di altre risorse all'interno dell'organizzazione per creare e mantenere una migliore struttura di controllo interno.

Il controllo interno è stato, e probabilmente sarà ancora, la chiave per una struttura aziendale vincente, oltre che un obbligatorio adeguamento alla normativa SOX. Esso è un processo effettuato dal consiglio di amministrazione dell'azienda, dal management e da altro personale che guida il successo aziendale in tre categorie:

- efficacia ed efficienza delle operazioni;
- affidabilità dell'informativa finanziaria;
- conformità alle leggi e ai regolamenti applicabili.

Sarbanes-Oxley affida esplicitamente ai CEO ed ai CFO la responsabilità di stabilire, valutare e monitorare l'efficacia del controllo interno sull'informativa finanziaria. Le proposte della SEC che hanno effetto su Sarbanes-Oxley, sono innegabilmente complicate e l'implementazione prevede un percorso lungo e costoso. Dalla sua introduzione, la semplice opinione espressa in buonafede, riguardo l'ultima revisione contabile, non è più sufficiente, in quanto non è una prova dell'efficacia del controllo interno. Sono queste le motivazioni che hanno dato il via all'incremento persistente di affidarsi a società di revisione.

I revisori indipendenti sono tenuti a esprimere un parere sul bilancio, senza dover però attestare la struttura di controllo interno, motivo per cui, le procedure di verifica che eseguono non sono progettate per soddisfare i requisiti di attestazione. Affinché il revisore indipendente possa effettuare tale attestazione, permettendo all'azienda di preparare la valutazione, è necessario adottare un quadro di controllo interno che contenga criteri oggettivi misurabili e valutabili.

La valutazione da fornire ai revisori indipendenti deve essere sostanziale, ben documentata e completa. Una lista di controllo abbreviata può includere:

- informazioni sull'ambiente di controllo complessivo della società;
- descrizione del processo intrapreso dal management per identificare, classificare e valutare i rischi che impedirebbero alla società di raggiungere obiettivi di informativa finanziaria;

- 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;
- risultati e documentazione di base dell'ultima valutazione del management sulla progettazione e sull'efficacia operativa delle singole attività di controllo;
- 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;
- descrizione del processo di creazione dell'informativa e delle relative attività di controllo.

Preso atto che informazione e dati hanno ruoli di fondamentale importanza, è implicito che lo abbia anche la Tecnologia dell'Informazione, ovvero l'IT.

Fortemente integrato nei processi aziendali, l'IT, rappresenta il mezzo di trasporto per dati e informazioni sia verso l'esterno che all'interno dell'azienda stessa. Più propriamente l'IT rappresenta "tecnologie riguardanti i sistemi integrati di telecomunicazione, i computer, le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare informazioni".[24] Non è difficile immaginare quanto sia fondamentale per un'azienda avere un solido sistema IT, che permetta una corretta assimilazione dei dati e una altrettanto fluida trasmissione degli stessi. Come descritto nel paragrafo 1.4, per quanto riguarda il soddisfacimento delle sezioni 404 e 302, sono previste rendicontazioni periodiche con conseguenti movimentazioni virtuali di enormi quantità di dati. Un sistema di Information Technology deve essere pertanto ottimizzato in modo da garantire prestazioni all'altezza. Questo implica sicuramente grossi investimenti per 'parti' di azienda di cui, prima dell'avvento della SOX, non si conosceva nemmeno l'esistenza.

Nel Giugno del 2004 entrò in vigore uno standard che stabilì dei criteri per cui un IT potesse essere considerato valido ai fini di un controllo SOX. Si tratta dell'Auditing Standard No.2, "an audit of internal control over financial reporting performed in conjunction with an audit of financial statements", così descritto in un report del PCAOB stesso, entrato in vigore il 17 giugno 2004. Questo lungo standard fornisce obblighi professionali e correlati orientamenti di gestione sull'audit e attestanti la valutazione da parte della direzione dell'efficacia dei controlli interni di un'impresa pubblica.

[24] Definizione tratta dall'Enciclopedia Treccani

"Sia il personale della SEC che quello del PCAOB sono tenuti, nel prossimo futuro, a fornire indicazioni su argomenti come i seguenti:

- acquisizioni recenti;
- società controllate consolidate ma non controllate;
- partecipate;
- qualificazione della relazione sui controlli interni;
- periodi di transizione;
- obblighi di informativa relativi a carenze significative e modifiche sostanziali apportate ai controlli interni;
- tempistica di valutazione del controllo interno sull'informativa finanziaria in relazione a determinati soggetti esteri".[25]

L'Information Technology iniziava così ad essere ufficialmente riconosciuta per l'importanza del suo operato. Le procedure standard richiedevano che le aziende analizzassero il modo in cui utilizzare l'IT per i processi finanziari, regolamentandolo affinché si riducessero i rischi ad esso associati.

[25] Tratto dalla documentazione ufficiale del PCAOB subito dopo l'introduzione della SOX

1.7 BREVE CONFRONTO CON LA NORMATIVA ITALIANA

In Italia gli aspetti societari e organizzativi sono trattati dalla legge per la tutela del risparmio (GU Serie Generale n.301 del 28/12/2005 – Suppl. Ordinario n.208). Anche in Italia, come in America, questa legge è stata emanata in conseguenza di scandali finanziari, quali Cirio e Parmalat. Nonostante gli aspetti trattati in questa normativa siano molteplici, è interessante raffrontare l'ambito di Corporate Governance e di responsabilità aziendale, con il Sarbanes-Oxley Act americano. La legge n°262 ha introdotto numerose novità in materia di governance, all'interno delle società italiane. Sono particolarmente interessanti le disposizioni introdotte in tema di responsabilità e obblighi relativi all'informativa societaria, in analogia con quanto introdotto dalle sezioni 302 e 404.

Di seguito si riportano gli articoli affini con alcune sezioni della SOX descritte nel capitolo 1.5:

- Art.154-bis comma 2 TUF. Attestazione da parte del Dirigente preposto alla redazione dei documenti contabili societari che gli atti e le comunicazioni della società diffusi al mercato e relativi all'informativa contabile, anche infra-annuale, corrispondano alle risultanze documentali, ai libri ed alle scritture contabili. → Sezione 302 della SOX: CEO e CFO devono personalmente certificare la correttezza e la completezza dell'informativa finanziaria inclusa nel bilancio.
- Art.154-bis comma 3 TUF. Il dirigente preposto alla redazione dei documenti contabili societari predispone adeguate procedure amministrative e contabili per la formazione del bilancio di esercizio e, ove previsto, del bilancio consolidato nonché di ogni altra comunicazione di carattere finanziario. → Sezione 404 della SOX: "Internal Control Report" è necessario ai fini del soddisfacimento dell'atto, sia italiano che statunitense. Esso deve attestare la responsabilità del management nell'implementare e mantenere un'adeguata struttura relativa al controllo interno, in particolare nell'ambito del reporting economico finanziario.

- Art.154-bis comma 5 TUF. Attestazione, con apposita relazione, dell'adeguatezza e dell'effettiva applicazione delle procedure da parte degli organi amministrativi delegati e del Dirigente preposto alla redazione dei documenti contabili societari. Attestazione della corrispondenza del bilancio alle risultanze dei libri e delle scritture contabili secondo i regolamenti che saranno emanati dalla CONSOB. Gli atti e il bilancio della società estera controllata, allegato al bilancio della società italiana sono sottoscritti dagli organi di amministrazione, dal direttore generale e dal dirigente preposto alla redazione dei documenti contabili societari di quest'ultima, che attestano la veridicità e la correttezza della rappresentazione della situazione patrimoniale e finanziaria e del risultato economico dell'esercizio. Il bilancio della società italiana controllante è corredato da una relazione degli amministratori sui rapporti intercorrenti fra la società italiana e la società estera controllata. La relazione è altresì sottoscritta dal direttore generale e dal dirigente preposto alla redazione dei documenti contabili societari. → Sezione 906.

CAPITOLO II

L'IMPORTANZA DELLA REVISIONE PER UNA SOLIDA GOVERNANCE ICT

2.1 INTRODUZIONE

In questo capitolo si approfondisce perché oggi la revisione contabile è così importante ed è sempre più commissionata ad aziende terze.

Per comprendere il complicato meccanismo che regola questo mercato di servizi, è fondamentale partire dai problemi che coinvolgono il processo di revisione. Uno di questi è il rischio IT.

Il sistema informativo aziendale è quell'insieme di elementi che raccolgono, elaborano, memorizzano e distribuiscono dati ed informazioni a supporto delle attività aziendali, tra cui, nello specifico, quelle decisionali, di coordinamento e di controllo. I sistemi informativi, indispensabili ai fini del supporto aziendale, sono anche una parte fragile insidiata dai rischi operativi. Essi possono provocare grosse perdite economiche, se si verificano malfunzionamenti, errori di gestione o attacchi dall'esterno. Il rischio IT viene definito come "il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione"[26]. Il rischio IT grava in due diversi modi su un'azienda, esso può generare sia malfunzionamenti tecnologici, quindi rappresentare un rischio diretto, sia, indirettamente, con conseguenze irreparabili per i processi operativi aziendali.

Sottovalutare un aspetto tanto significativo può portare a gravi conseguenze all'interno della Governance ICT, per cui ad oggi, le organizzazioni sono sottoposte a controlli interni iterati e scrupolosi che possano garantire, l'integrità del trattamento dei dati e delle informazioni. Applicazioni e sistemi vengono sottoposti

[26] BANCA D'ITALIA, Nuove disposizioni di vigilanza prudenziale per le banche, luglio 2013

costantemente a test rigorosi in quanto anche un solo errore all'interno di un sistema informativo può essere sufficiente per esporre a ingenti perdite l'intera società.

Dagli scandali dei primi anni 2000 l'importanza dell'informativa societaria è in costante aumento. Il fine ultimo delle normative (quali la SOX) è quello di tutelare gli azionisti mitigando il rischio. È sempre più usuale osservare, all'interno di atti legislativi, articoli particolarmente specifici nei confronti di governance e gestione dei sistemi informativi aziendali.

Le organizzazioni IT si stanno rivelando indispensabili per operare in un ambiente sicuro. Esse rappresentano degli ottimi alleati per l'organizzazione strategica ed organizzativa; per poter adempire ai requisiti di governance, mitigazione del rischio e conformità, richiesti dalle leggi vigenti.

La valutazione del rischio IT è un processo non sempre immediato e attendibile al 100%. Il problema, inoltre, non si risolve semplicemente affidando la responsabilità a soggetti terzi quali assicurazioni. Affinché venga correttamente eseguita una gestione del rischio è di fondamentale importanza proteggere le informazioni fornendo adeguati rapporti di conformità. Un corretto trattamento del rischio prevede di coadiuvare strutture di business con le varie funzioni, in modo da tutelare anche il sistema informativo.

Definito il rischio IT, la rilevanza dei controlli e la complessità per svolgerli, chiariscono la necessità che le aziende hanno di affidarsi a team capaci di fornire valido supporto e spiega inoltre, perché i Team siano così richiesti dalle grandi organizzazioni; ma di cosa si occupano effettivamente queste società di supporto?

Gli audit esterni sono strutturati per verificare:

- La contabilità generale di un'azienda, oltre che determinare un quadro generale e reale della situazione di mercato e finanziaria. Quest'attività è fondamentale per prendere corrette decisioni manageriali.
- La validità dei registri finanziari, in quanto errori nei registri societari causati da frodi o appropriazioni indebite potrebbero causare il collasso di un'azienda. Si aumentata così la credibilità del bilancio e di conseguenza la fiducia degli investitori;

- La presenza di eventuali errori all'interno del sistema o altre attività fraudolente.

Gli audit esterni sono inoltre di grande aiuto nel portare, all'interno dell'organizzazione, conoscenze attuali tratte da esperienze globali.

2.2 LA REVISIONE, IL LATO DELL'OFFERTA

Il gruppo denominato "Big Four" rappresenta le aziende principali che si dividono il mercato della revisione e della consulenza ed è composto da:

- Deloitte
- Pricewaterhouse Coopers (PwC)
- Ernst & Young (EY)
- KPMG

In termini di dimensioni, dipendenti e fatturato, queste quattro società presentano indicativamente gli stessi numeri e hanno la maggiore influenza nel settore della contabilità e della revisione contabile, in particolare negli Stati Uniti dove controllano oltre l'80% delle società pubbliche.

I principali servizi di consulenza offerti riguardano gli ambiti Audit, Tax & Legal, Consulting/Advisory e altro (investigazione sulle frodi, acquisizioni, ecc..). Da anni la revisione contabile è uno dei servizi più offerti e tra i più remunerativi esistenti, ne sono causa anche le normative discusse nel capitolo precedente. Punto di forza di questo settore specifico è sicuramente il fatto che aver usufruito del supporto professionale da una di queste grandi aziende, dimostra trasparenza e garantisce fiducia da parte degli investitori; un tale impegno, quindi, risulta vantaggioso sia per chi offre la consulenza, sia per chi se ne avvale. Investire in revisioni contabili è pertanto una strategia vincente; nonostante i costi siano elevati, il guadagno che se ne ricava, sia in termini economici che di immagine, è di gran lunga superiore. Fornire informazioni accurate agli investitori è diventato una fonte di profitto. Di seguito vengono riportati i ricavi (Grafico 2.1) e il numero di dipendenti (Grafico 2.2) relativi all'anno fiscale 2021 per le Big Four.

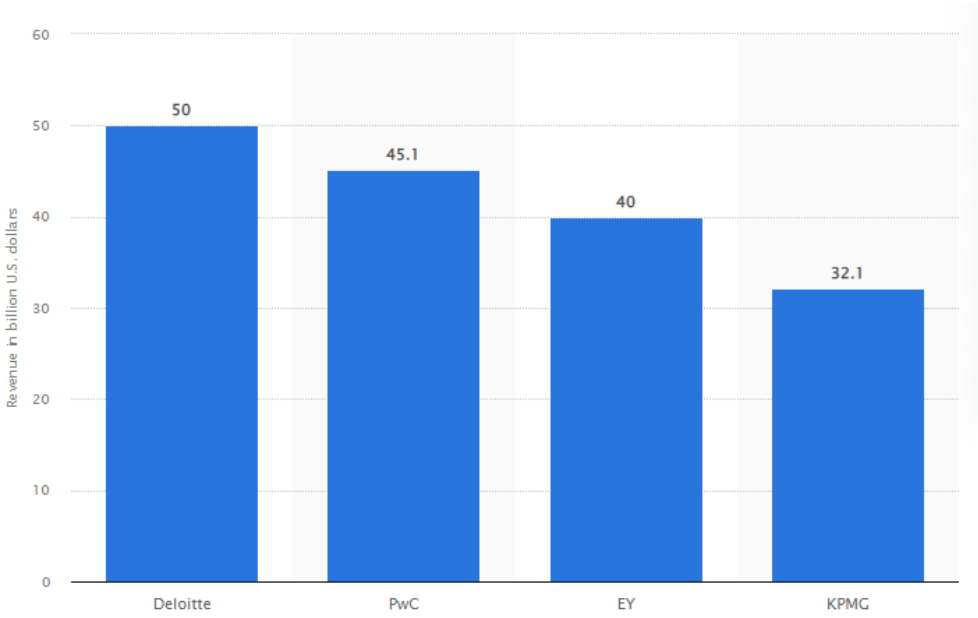


Grafico 2.1: Revenue of the Big Four accounting / audit firms worldwide in 2021. Fonte: Statista

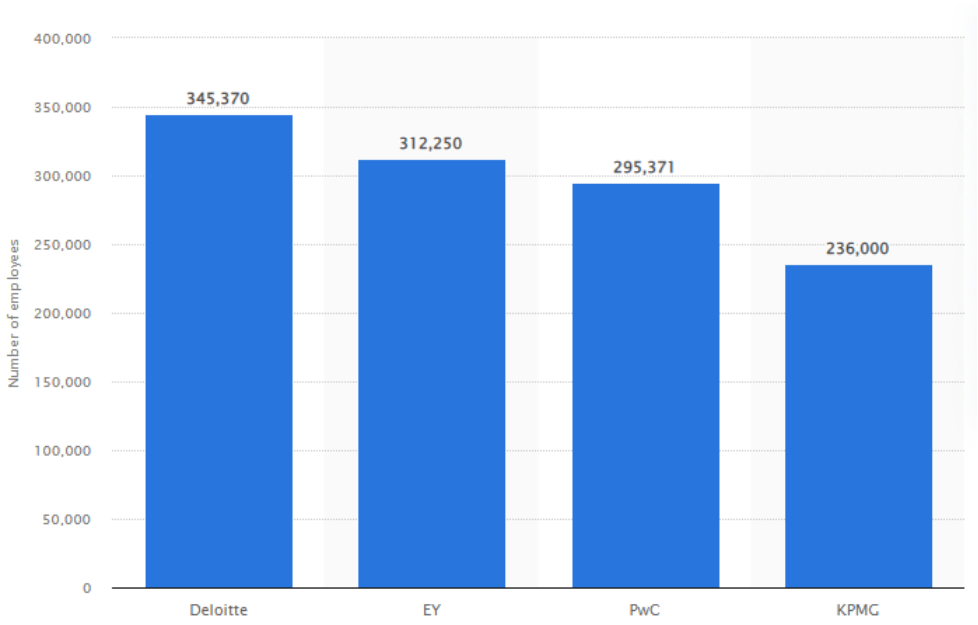


Grafico 2.2: Number of employees of the Big Four accounting / audit firms worldwide in 2021. Fonte: Statista

Se si pensa al bilancio, con relativi conti economici e patrimoniali, come la carta d'identità contabile di un'azienda, la società che svolge la revisione può essere considerata l'ente che ne redige il documento. Un importante aspetto da non sottovalutare nell'ambito della revisione, affinché il bilancio sia controllato efficacemente, è che l'azienda sia esterna.

"… il revisore, armato del dovuto scetticismo e dell'assoluta indipendenza, gioca un ruolo chiave che per legge dev'essere impermeabile a qualsiasi tipo di conflitto di interessi. In Italia, infatti, è in vigore l'obbligo di esclusività dell'oggetto sociale per le società di revisione. Tradotto: chi volesse offrire anche altri servizi diversi dalla revisione -ad esempio la consulenza in materia tributaria e fiscale- dovrebbe dar vita a società separate. È un requisito di indipendenza. E così accade, o dovrebbe accadere. "Non si può assistere qualcuno a scrivere un bilancio e poi verificare che quel lavoro sia stato fatto correttamente", sintetizza bene Gian Gaetano Bellavia, commercialista e consulente della Procura di Milano in materia di riciclaggio".[27]

Un altro grande rischio che influenza i bilanci societari è relativo alle asimmetrie informative. Questi problemi possono appartenere a due diverse categorie:

- Informazione nascosta. Si ha quando non viene rivelata un'informazione privata che avrebbe potuto influenzare delle decisioni, sia in modo positivo che in modo negativo. Questa asimmetria informativa necessita di test di controllo, affinché la parte non informata induca l'altra a rivelare tali informazioni.
- Azione nascosta. Avviene nel momento in cui una parte tende a falsare e/o nascondere una propria iniziativa che potrebbe essere conseguenza di cambiamenti, positivi o negativi, che cambierebbero un'opinione o una decisione. In un ambiente economico la soluzione in questi casi è quella di stabilire degli incentivi che scoraggino queste azioni.

[27] Tratto da un articolo di altreconomia.it: '*Bilanci e consulenza: in Italia il mercato è in mano alle "Big four"'* del 1°Aprile 2018

La revisione esterna dei rendiconti contabili e finanziari nasce proprio dall'esigenza degli azionisti di far verificare, da un'entità terza, l'effettiva assenza di queste asimmetrie informative, che potrebbero, potenzialmente, indurre a un fallimento di mercato.

Incentivi e monitoraggi, se eseguiti internamente, rischiano di essere falsati e di soffrire delle stesse asimmetrie che dovrebbero risolvere e per cui vengono introdotti. Come in un circolo vizioso, i problemi di informazione e azione nascosta si espandono all'interno dei processi aziendali. Affinchè le informazioni contabili non siano sottoposte ad azioni di corruttibilità, Il controllo interno non può essere effettuato unicamente dalle aziende. Il rischio sarebbe di dare la possibilità ai revisori interni di manipolare e modificare i dati per scopi diversi da quello del controllo.

Falsare il bilancio non significa semplicemente aggiungere o togliere uno zero da una voce contabile; errori contabili provocano ulteriori conseguenze altrettanto gravi, come per esempio criticità gestionali, economiche e finanziarie o informazioni distorte dei manager sulle reali prospettive societarie.

Il modello economico che studia questi comportamenti è conosciuto come 'approccio principale-agente' [28] e regola il rapporto tra "controllore" e "controllato". Viene definito come una "relazione di agenzia che si determina quando l'esito di un accordo contrattuale per una parte dipende dal comportamento dell'altra, in cui l'agente (o mandatario) è il soggetto che agisce; il principale (o mandante) è il soggetto su cui incide l'azione dell'agente."[29]

Questa teoria si basa sui problemi di informazione nascosta che questo rapporto determina; occorre che l'agente faccia qualcosa, ma il principale non può controllare lo sforzo effettivo. Appare evidente quindi che il controllore ed il

[28] Approccio Principale-Agente, Tirole 2014
[29] Definizione dell'enciclopedia Treccani dal dizionario di economia e finanza

controllato non possano appartenere alla stessa società; per questo motivo è necessario ricorrere a una revisione esterna con un rapporto di agenzia.

Un rapporto di agenzia si basa su uno schema di incentivi dati dal principale all'agente, affinché quest'ultimo sia meno incline a nascondere azioni o informazioni. È quello che avviene quando una società paga una consulenza che ha il compito di revisionare il sistema di controllo interno. Sono due i nuovi harmful effects:

- Gli incentivi hanno ovviamente un costo, ed esso dipende dall'avversione al rischio dell'agente;
- Anche le società che svolgono consulenze esterne devono essere controllate.

Il PCAOB, descritto precedentemente, rappresenta l'organo giuridico che "controlla il controllore", assicurandosi che vengano adempite tutte le direttive del Sarbanes-Oxley Act. Le aziende sono tenute a disporre di una governance e soprattutto di un framework di riferimento adeguati, in modo da garantire una diminuzione dei rischi di non conformità ed etici.

2.3 IL COSO FRAMEWORK

Per continuare l'analisi è necessario richiamare le definizioni assegnate dalla bibliografia attuale, al termine adeguatezza. Questo termine, spesso associato al concetto di conformità, rappresenta la capacità, intesa in termini aziendali, di gestione dei rischi che si presentano nel tempo e le relative azioni che vengono intraprese ai fini della mitigazione degli stessi. Un esempio può essere dato dall'adozione di un sistema di controllo, atto a stabilire una certa stabilità nei processi aziendali.

Ai sensi del D.Lgs. 231/01 è richiesta l'adeguatezza del sistema di controllo interno e della relativa gestione dei rischi, pena la responsabilità primaria del Consiglio di Amministrazione (CdA). "La conformità al Sarbanes-Oxley Act non crea tuttavia un ambiente privo di rischi, che di fatto non esiste. Conformarsi ad esso ed avere una corretta governance dell'IT aiuta ad ottenere report finanziari più tempestivi ed accurati".[30]

Una soluzione al complesso iter riguardante la gestione e la valutazione del sistema di controllo interno può essere quella, sposata dalla maggior parte delle aziende obbligate a sottostare alla normativa SOX, di fare riferimento a dei framework standard. Il processo di controllo, infatti, per quanto intricato e lungo, può essere ricondotto a procedimenti standard e talvolta ricorsivi. Il "COSO Framework" rappresenta il framework più diffuso in questo ambito. Il Committee of Sponsoring Organizations of the Treadway Commission (COSO) suddivide il controllo interno in cinque componenti interconnesse:

- "Ambiente di controllo - il fondamento di tutti gli elementi del controllo interno, che include i valori etici e la competenza dei dipendenti dell'azienda;
- Valutazione del rischio - l'identificazione e l'analisi di rischi rilevanti che possono ostacolare il raggiungimento degli obiettivi aziendali;

[30] *Obiettivi di controllo IT per il Sarbanes_Oxley Act*, 2° Edizione, settembre 2016

- Attività di controllo - compiti specifici per mitigare ciascuno dei rischi identificati;
- Informazione e comunicazione - percorsi informativi dal management ai dipendenti e viceversa;
- Monitoraggio - la determinazione e la valutazione del controllo interno".[31]

Si rappresenta di seguito in Figura 2.1 il processo del ciclo del COSO Framework, riassuntivo del percorso da intraprendere per una corretta gestione dei rischi, nonché i cinque elementi che rappresentano la struttura portante del COSO Framework.

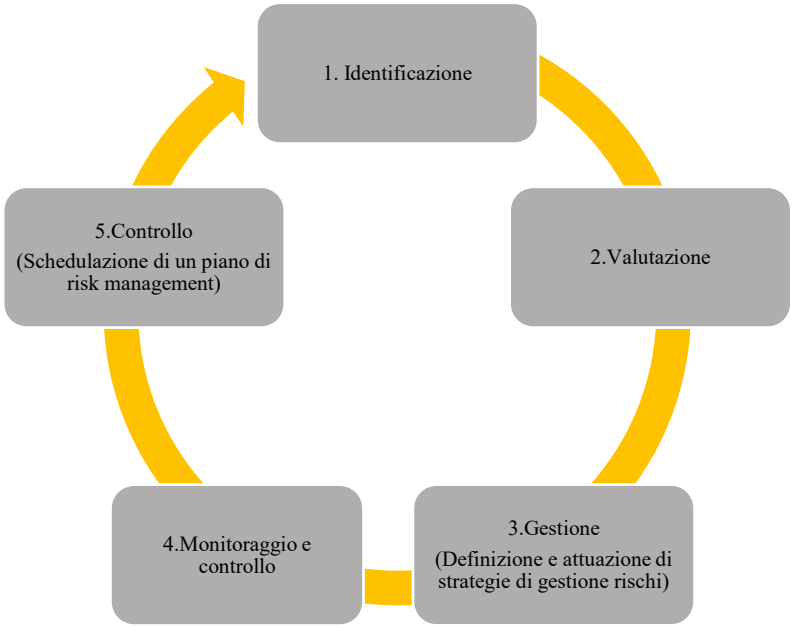


Figura 2.1: Struttura del COSO Framework

Obiettivo primario del COSO è quello di fornire un modello univoco che sia da riferimento comune per tutte le parti interessate al controllo interno aziendale.

[31] Elenco estrapolato da 'Guide to Improving Corporate Governance, Deloitte & Touche, 2003'

Rappresenta uno strumento utile per soggetti sia interni che esterni all'organizzazione, quali investitori, potenziali acquirenti o qualunque stakeholder.

Come riporta il COSO, il sistema di controllo interno è: "A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance".

Un ambiente di controllo correttamente integrato, basato su principi etici, con un corretto sistema sanzionatorio e politiche di incentivazione garantisce un'organizzazione vincente.

Andando più nello specifico per quanto riguarda le attività di controllo, il compito ulteriore di una società è quello di giudicare la sicurezza IT attraverso analisi specifiche quali:

- Verifiche nel dettaglio del disegno e dell'operatività dei controlli:
    - Test dei controlli automatici (ITAC);
    - Analisi sulle interfacce e sui datawarehouse;
    - Analisi delle informazioni fornite dall'Entity (IPE);
    - Test sui General Information Technology Controls (ITGC):
        1. Change Management;
        2. User Access Management;

- Mappatura degli applicativi utilizzati dall'azienda.

Un altro aspetto importante del COSO è rappresentato dalla componente "Information & Communication", con cui l'organizzazione si pone l'obiettivo di redigere la documentazione necessaria in date fissate, con costanza periodica, rivolgendosi sia agli interlocutori esterni che interni tramite la condivisione degli obiettivi del sistema di controllo stesso e i risultati del Risk Assessment.

Un ulteriore ruolo di grande importanza, ai fini della credibilità della revisione, è ricoperto dalle certificazioni ISO per la qualità e il controllo sulla produzione.

Queste, devono essere costantemente valutate e verificate per garantire il corretto funzionamento del sistema di controllo interno. Viene di seguito riportata una rappresentazione grafica intuitiva del COSO framework (Figura 2.2).

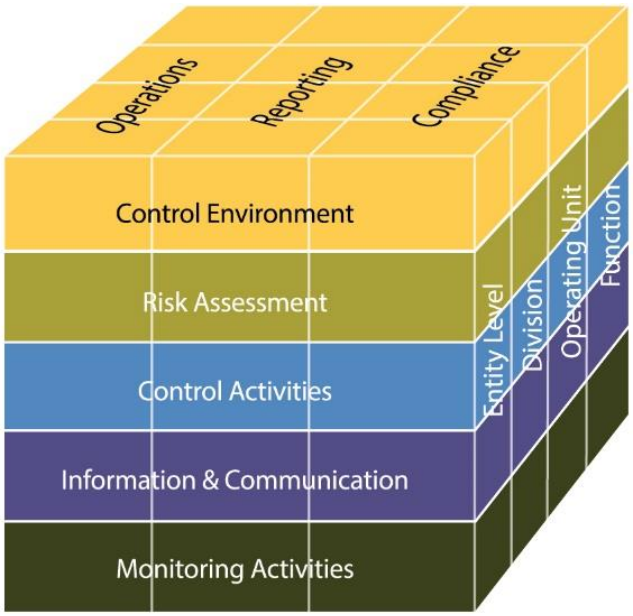


Figura 2.2: Rappresentazione del COSO framework.

Seguire un framework quale COSO è necessario ai fini della conformità alla Sarbox. Per capire cosa effettivamente migliori in termini di Governance la Figura

2.3 illustra quanto il valore di business di un'azienda cambi in funzione della conformità alla normativa SOX; in particolare è esplicitato come il valore di business sia direttamente proporzionale al soddisfacimento delle seguenti attività:

1. Pianificazione e definizione del perimetro dei controlli IT;
2. Valutazione i rischi;
3. Documentazione dei controlli: ITGC, ITAC, IPE;
4. Valutazione del disegno dei controlli e dell'efficacia operativa;
5. Valutazione delle priorità;
6. Costruzione della sostenibilità.

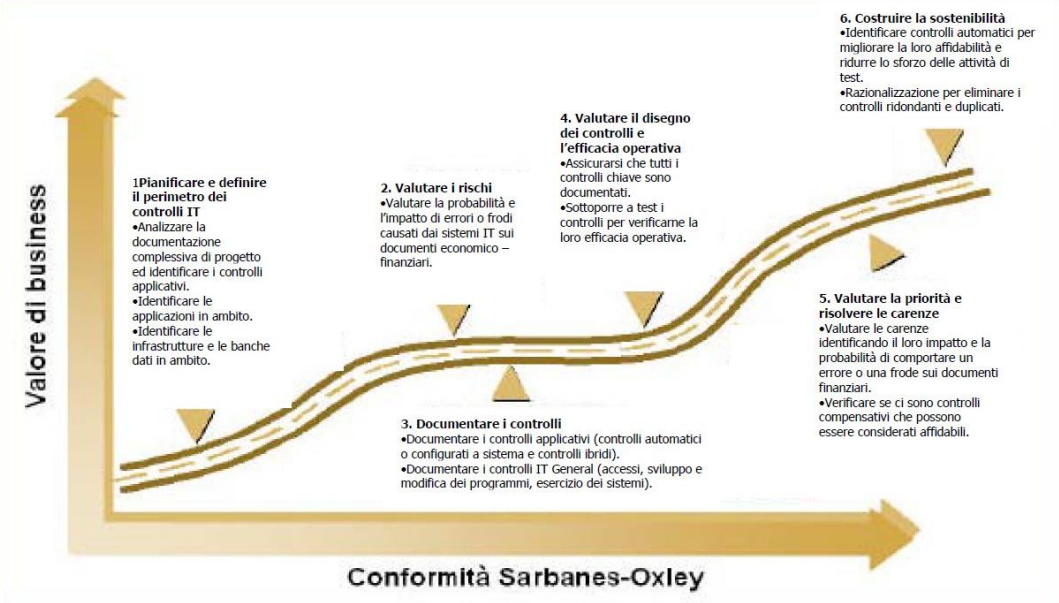


Figura 2.3: Mappa per la conformità IT. Fonte: Obiettivi di controllo IT per il Sarbanes_Oxley Act, 2° Edizione, settembre 2016

2.3.1 LA ISO 27001

L'attività degli audit IT è costituita in gran parte dal perseguimento di standard, requisiti e regolamenti imposti, indipendentemente dal tipo di organizzazione settore o ambiente operativo. Una normativa molto importante nel contesto di revisioni contabili è la normativa ISO 27001.
La ISO 27001, conosciuta anche come Information Security Management System (ISMS), è una normativa internazionale introdotta nell'ottobre 2005.

La conformità alla ISO27001 è un requisito facoltativo, ma molto richiesto nei rapporti con fornitori o partner commerciali. Essa certifica la corretta gestione dell'IT security all'interno dell'organizzazione. Il framework ISO 27001 fornisce un modello da seguire durante la configurazione e il funzionamento del sistema di gestione; tutela la sicurezza delle informazioni e dei dati, analizzando i problemi ad essi legati lungo tutto il percorso che porta alla loro acquisizione.

Parallelamente al framework COSO la ISMS aiuta a identificare, valutare e mitigare i rischi informativi a cui si può andare incontro all'interno di un sistema informativo. La normativa, pur non imponendo alcun controllo formale, garantisce l'allineamento costante e ottimizzato delle disposizioni vigenti in materia di sicurezza. La ISO27001 fornisce un elenco di 35 obiettivi di misura (controlli) per identificare misure concrete a vantaggio della sicurezza informativa.
Le organizzazioni che adottano questa normativa hanno facoltà di scegliere, da un paniere di controlli, quelli più adatti alle specifiche del loro contesto e i rischi ad esso associati. Per definire correttamente i controlli da intraprendere è quindi opportuno eseguire una valutazione dei rischi, attività che viene effettuata nella fase di risk assesment. Questa valutazione prevede un'analisi sull'ambiente e sull'organizzazione IT dell'azienda, al fine di poter individuare le criticità che potrebbero corrompere la sicurezza delle informazioni.

I rischi non potranno essere eliminati completamente; tra l'altro le aziende non sempre perseguono la scelta di utilizzare risorse e tempo, potenzialmente destinabili ad altro. Una strategia aziendale potrebbe essere quella di intraprendere una strada più o meno avversa al rischio. Possibili scelte potrebbero essere quelle di evitare, condividere o accettare determinati rischi, piuttosto che mitigarli attraverso i controlli.

2.4 I CONTROLLI: ITGC, ITAC, ITDM

Approfondendo maggiormente il meccanismo revisionale, è interessante osservare i controlli effettuati nello specifico. Essi rappresentano il cuore della revisione contabile.

2.4.1 ITGC

Gli Information Technology General Controls (ITGC) sono una tipologia di controlli che interessano l'ambiente in cui sono sviluppati i sistemi IT. Essi identificano un quadro generale di verifica delle attività IT, e seguono procedure e policies per poter supportare correttamente il funzionamento delle applicazioni, garantendo l'integrità dei report generati.

Attraverso questa tipologia di controlli, viene effettuata una analisi iniziale per stabilire una base di sicurezza generale valida per tutto il corso della gestione di un sistema informatico.

In particolare, è necessario verificare:

- La **riservatezza** di informazioni e dati per garantire protezione da possibili divulgazioni intenzionali e non;
- L'**accuratezza** di informazioni, dati e transazioni che vengono utilizzati durante il controllo;
- La **completezza** delle informazioni ottenute dal processamento dei dati.

Durante un ITGC vengono coinvolti due differenti layer: un layer infrastrutturale, relativo ai supporti generali di tutti gli applicativi (sistema operativo e database) e un layer applicativo, proprio della gestione di un sistema informativo.

Le aree su cui agiscono gli ITGC si differenziano in Manage Access, Manage Change e Manage IT operations.

All'interno del **Manage Access** sono individuati gli ITGC che verificano gli accessi all'ambiente IT. Questi analizzano la corretta appartenenza delle utenze all'interno di un determinato applicativo o software, in modo da impedire azioni potenzialmente rischiose da parte di users che non hanno le autorizzazioni necessarie per intraprenderle.

Nel **Manage Change** intervengono i controlli relativi a modifiche, aggiornamenti e/o manutenzioni da apportare agli applicativi IT o ad altri componenti interni all'environment IT.

I controlli effettuati direttamente sulle applicazioni di archiviazione e di elaborazione dati, per verificare che le informazioni trattate non siano state soggette a fenomeni di corruttibilità o manipolazione, rappresentano invece l'area **Manage IT Operations**.

Si riporta di seguito, uno studio sull'effettivo funzionamento dei controlli all'interno delle 3 aree.

L'obiettivo dei Manage Access è quello di identificare una struttura organizzativa con ruoli ben definiti, in cui siano rispettate le responsabilità relative alle varie utenze. I controlli riscontrabili nell'area di Manage Access sono relativi a:

- Processi di crezione/modifica utenze, con relativo test su tutto il processo di autorizzazioni;
- Password Policy, in cui è prevista la verifica del livello di sicurezza adottato, e la congruenza con le policy di audit vigenti spesso associati a standard;
- Verifiche sull'effettiva eliminazione di utenze relative a personale dimesso o escluso per altri motivi;
- Analisi Segregation of Duties (SoD), che riguarda la valutazione della corretta segregazione delle funzioni, in quanto è necessario che, i processi di modifica o creazione utenze siano stati effettuati da persone diverse rispetto a quelle valutate. In sostanza rappresenta la verifica che un ente non sia valutato da sé stesso.

All’interno del processo di Manage Change sono individuati quattro tipologie di cambiamenti:

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

Le modifiche effettuate individuano anche il livello di rischio ad esse associate, che ovviamente varia a seconda della priorità che detiene la modifica. Le possibili casistiche in cui si può ricadere in funzione del livello di rischio sono tre:

- Applicativi IT o modifiche effettuate sui programmi esistenti non funzionanti come richiesto in quanto non testati dalla persona con le competenze adatte;
- Modifiche apportate non dal personale autorizzato;
- SoD (segregation of duties) non rispettata correttamente.

Per ultimi, i processi di Manage IT Operations, individuano la parte di programmazione e di monitoraggio sui lavori (job), compresa l'accettazione dei dati e l'interfaccia. Questo processo è tipicamente rilevante quando vengono trattati job che fanno parte del percorso critico delle SCOT[32]. Il dipartimento IT (al contrario degli utenti aziendali) è responsabile dell'avvio e del monitoraggio dell'elaborazione dell'applicazione IT. Il fine ultimo di questa parte di processi è quello di verificare che l’azienda da revisionare abbia un ambiente di elaborazione dati affidabile. Per effettuare questa analisi è necessario effettuare controlli sulle applicazioni utilizzate per ottenere i backup delle informazioni, verificando che funzionino in maniera adeguata. Per i Manage IT Operations è necessario verificare che l’accesso alla schedulazione dei job sia consentito solo al personale autorizzato, che i backup vengano effettuati con una frequenza periodica stabilita e che ci sia una corretta gestione automatica dei job.

[32] SCOT: significant class of transaction, ovvero le voci di bilancio che maggiormente incidono sui conti di una società

2.4.2 ITAC e ITDM

Per ottenere un'analisi più accurata e completa dei processi di business della società revisionata, si effettuano ulteriori controlli sui vari applicativi, per prevenire transazioni non autorizzate e per supportare il processo di auditing del bilancio.

In particolare, vengono definiti due ulteriori categorie di controlli (Figura 2.4):

- Gli IT Application Control (ITAC), controlli sugli applicativi eseguiti in modo automatico privi di alcun tipo di intervento manuale;

- Gli IT Dependent Manual, controlli ibridi, comprensivi di una componente manuale e una automatica.

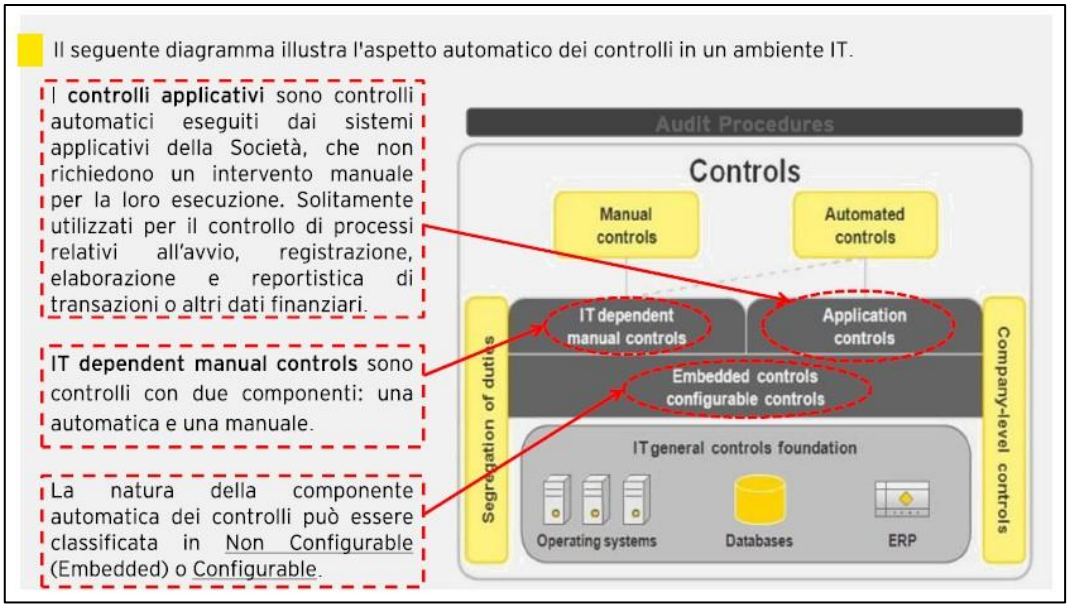


Figura 2.4: Rappresentazione di ITDM e ITAC

Gli ITAC rappresentano controlli incorporati all'interno dei sistemi applicativi stessi, in quanto vengono definiti da qualunque automatismo identificato nel sistema. Questa tipologia di controllo può includere algoritmi automatici, impostazioni configurabili, estrazioni automatiche di dati e calcoli generali automatici. Il test ha il fine di verificare se queste funzioni vengono correttamente implementate.

Vengono di seguito riportati alcuni esempi di controlli ITAC:

- Fixed Assets, algoritmi che permettono il calcolo automatico di spese di ammortamento;

- Account payable, parte di gestione dell'approvazione da parte degli enti autorizzati agli ordini d'acquisto;

- Sales/Account receivable, blocco degli ordini dei clienti in caso di superamento del limite massimo di credito.

Gli ITDM sono invece controlli di natura biunivoca, in quanto sono costituiti da componenti sia manuali che automatiche. Sono caratterizzati dalla presenza di report generati automaticamente da sistema, detti IPE, che forniscono la documentazione utile ai fine della revisione contabile da parte del management.

La valutazione dei crediti verso i clienti rappresenta un controllo di tipo ITDM. Per verificare l'adeguatezza di questa tipologia di controllo, il revisore, consulta manualmente il database con le scadenze periodiche, estratta automaticamente dal sistema, per verificarne l'appropriatezza.

2.5 COME IDENTIFICARE UN PROCESSO IT

Un'organizzazione è in grado di gestire il proprio ambiente IT attraverso l'utilizzo di processi informatici. Un processo informatico è rappresentato dall'insieme di attività svolte per garantire all'ambiente IT il soddisfacimento delle esigenze dell'azienda (apportare una modifica al software, fornire/rimuovere l'accesso di utenze, monitorare il funzionamento dei programmi informatici). La maggior parte delle attività di processo sono rappresentate dagli ITGC.

Come già detto in precedenza, i processi informatici più rilevanti possono essere riassunti all'interno delle tre macrocategorie Manage Access Processes, Manage Change Processes e IT Operations Processes.

Ulteriori processi informatici possono essere rilevanti a seconda dell'uso dell'IT da parte dell'entità, compreso il modo in cui essa gestisce le operazioni dei componenti dell'ambiente IT (ad esempio, eseguire la programmazione dei lavori e monitorarne l'elaborazione). L'obiettivo comune di questi processi è quello di garantire e mantenere la sicurezza e l'integrità dei dati trattati e di gestire l'accesso ai componenti dell'ambiente IT.

Un corretto approccio alla comprensione dei processi informatici in ambito revisionale si concentra sulla determinazione dell'esistenza di condizioni che influiscano sull'adeguatezza del processo informatico per la gestione dei rischi generali per il bilancio (ossia, il rischio che le applicazioni informatiche non elaborino in modo coerente e accurato gli SCOT e gli FSCP[33] e/o il rischio che non venga mantenuta l'integrità dei dati utilizzati negli stessi).

Per gli audit sull'affidabilità dei controlli, si considerano i processi IT; essi individuano i rischi specifici associati alle modalità con cui vengono effettuati. Occorre quindi implementare ITGC per affrontare correttamente tali rischi informatici.

[33] **FSCP** (*financial statement close process*): processo di chiusura del bilancio, trasforma le operazioni, e le informazioni su eventi o condizioni diversi dalle operazioni, presenti nella contabilità e nelle altre registrazioni di supporto di un'entità in un bilancio e nella relativa informativa.

Per poter garantire una corretta revisione contabile, che sia chiara e al contempo efficace, è fondamentale che all'interno di un'organizzazione non venga mai meno la comprensione delle tecnologie dell'informazione e il loro ruolo. L'utilizzo di IT implica che vengano alterate nelle fasi di inserimento, elaborazione, conservazione e rendicontazione molte informazioni rilevanti del bilancio. È quindi importante che l'entità presti attenzione nell'uso dell'informatica in quanto essa influisce su:

- Strategia generale di revisione;
- Valutazione dei rischi;
- Definizione delle procedure di revisione.

Il principale strumento informatico, ad oggi di gran lunga più diffuso in questo ambito, è senza dubbio Microsoft Excel. Viene utilizzato principalmente per guidare l'entity in operazioni commerciali e finanziare, e direttamente per il cliente finale.

Altre applicazioni informatiche commerciali sono utilizzate a seconda delle esigenze dei clienti e dei controlli specifici alle circostanze. Queste applicazioni "off-the-shelf", solitamente concesse per periodi di tempo stabiliti da una licenza, non sono personalizzabili e vengono definite "vendor supplied".

Talvolta un'applicazione può essere sviluppata internamente dall'organizzazione che cura un cliente con delle specifiche non riconducibili a nessun altro caso esistente e/o precedentemente trattato. Il cliente avrà quindi l'esclusiva per l'utilizzo di questa applicazione.

L'ultima categoria di applicativi comprende tutti i software contenenti applicazioni informatiche complesse, pre-programmate e di base standard per tutti, ma configurabili. Un esempio può essere il software SAP.

Si elencano le fasi che devono essere impiegate per un corretto uso dell'IT da parte dell'entità.

1. Capire in che misura il modello di business integra l'uso dell'IT;
2. Stabilire quanto l'effetto dell'IT possa impattare sulle componenti del sistema di controllo interno a livello entity;
3. Comprendere le classi significative di operazioni (SCOT), i sottoprocessi del processo di chiusura del bilancio (FSCP), identificare quindi le applicazioni informatiche rilevanti per la revisione;
4. Identificare il materiale necessario, appartenente all'IT environment (come sistemi operativi, database, software di rete), a supporto delle applicazioni utilizzate;
5. Effettuare previsioni su quanto i processi IT influenzano la strategia di revisione e i rischi di errori significativi a livello di bilancio;
6. Per i processi IT, relativi ai componenti rilevanti dell'ambiente, che supportano il funzionamento dei controlli, vengono identificati i rischi IT specifici e gli ITGC ad essi associabili. Per gli ITGC identificati ne viene quindi valutata l'efficacia progettuale e se sono stati implementati;
7. Verificare l'efficacia operativa degli ITGC attraverso test, utilizzando i risultati dei controlli come base per valutare i processi IT a cui fanno riferimento. Quando gli ITGC sono inefficaci, possono essere identificati ITGC supplementari o eseguire procedure IT aggiuntive per affrontare i rischi IT interessati;
8. Eseguire procedure di aggiornamento appropriate fino alla fine del periodo relativo al controllo.

A volte situazioni o clienti particolari richiedono l'inclusione all'interno del team che segue l'iter sopra descritto di professionisti esperti, in modo da garantire una migliore comprensione delle problematiche legate all'IT e una corretta interpretazione di ambienti IT estremamente complessi.

2.6 RISCHI LEGATI AI PROCESSI IT

Come già sottolineato in precedenza, l'IT non è un ambiente privo di rischi. Attraverso un'analisi atta a identificare criticità legate all'utilizzo dell'IT emerge che, le applicazioni informatiche, possono elaborare dati in modo impreciso. Questo implica un malfunzionamento e, pertanto, l'elaborazione coerente e accurata degli SCOT o del FSCP è a rischio. L'integrità stessa dei dati può essere compromessa. In ambito di revisione questi rischi possono essere affrontati diversamente a seconda della strategia di audit che si intende intraprendere.

Fully substantive audits

Quando viene utilizzata una strategia di revisione full substantive, per le applicazioni informatiche rilevanti ai fini della revisione, occorre indentificare e comprendere i componenti dell'ambiente informatico di supporto e i processi informatici dell'entità. Questa conoscenza aiuta a determinare se i processi di protezione e gestione dell'ambiente informatico dell'entità creino rischi di inesattezze significative che vengono affrontate attraverso le procedure sostanziali. Per riuscirci occorre procedere seguendo i seguenti step:

1. Identificare il critical path delle SCOT e dei sottoprocessi dell'FSCP includendo le applicazioni utilizzate per supportarli;
2. Identificare i componenti dell'ambiente IT di supporto e i processi IT che supportano le applicazioni IT identificate;
3. Comprendere i processi IT rilevanti;
4. Rispondere alle circostanze identificate che indichino l'inadeguatezza dei processi IT per affrontare il rischio.

Quando viene constatata l'esistenza di condizioni che corrompono l'adeguatezza del processo IT, è prevista un'ulteriore richiesta al management per allinearsi sulla strategia da perseguire ai fini della mitigazione dei rischi IT; in particolare, è necessario capire se tali controlli di mitigazione possono essere attuati tramite SCOT o FSCP. Se nelle SCOT o nell'FSCP non vi sono controlli che affrontino il

possibile effetto dei relativi rischi informatici sul bilancio, viene dichiarata l'esistenza di una carenza ITGC.

Controls reliance audits

Quando viene utilizzata una strategia di reliance dei controlli per gli SCOT o l'FSCP, occorre identificare le applicazioni IT, i componenti dell'ambiente IT di supporto e i processi IT. Viene richiesto quindi uno studio dei rischi informatici dell'esecuzione di tali processi e i relativi ITGC che affrontano tali criticità quando ci sono controlli applicativi. Inoltre, è opportuna la verifica dell'effettiva efficacia operativa degli ITGC progettati.

Queste procedure sono il punto di partenza per determinare se può essere fatto affidamento sui processi IT.

Se un ITGC viene definito inefficace, può essere identificato e testato un ITGC compensativo, o implementata una nuova procedura sostanziale IT, per affrontare il rischio correlato al fine di sostenere l'affidabilità dei processi IT. Quando è invece possibile fare affidamento sui processi IT, questi supportano il funzionamento degli applicativi e sostengono il mantenimento dell'integrità dei dati utilizzati in tali controlli.

Un'ulteriore categoria di strategie è rappresentata dalle cosiddette strategie di audit ibride. Esse vengono attuate nel caso in cui venga fatto affidamento a una strategia di reliance per alcuni controlli SCOT o FSCP e una strategia full substantive per altri. L'approccio volto alla comprensione dei processi IT si basa su alcune guide relative sia alle casistiche di strategie di reliance che di fully substantive.

Al fine di introdurre il caso studio elaborato durante l'esperienza di tirocinio, vengono affrontati i rischi relativi ai Manage Access processes, esaminati per la quasi totalità dell'esperienza curriculare in ambiente aziendale.

2.6.1 IL RISCHIO LEGATO ALLA RICONVALIDA DELL'UTENTE

I controlli che vengono eseguiti per gestire gli accessi a un determinato applicativo costituiscono parte dei Manage Access processes. Atti a gestire l'accesso ad applicazioni informatiche, dati e altri componenti dell'ambiente IT, essi verificano la validità delle impostazioni di sicurezza e l'effettiva idoneità dei soggetti a cui vengono concessi i diritti d'accesso (direttamente o attraverso ruoli e privilegi di accesso associati allo user in questione).

Per eseguire una corretta riconvalida delle utenze è necessario avere informazioni riguardanti il database contenente la popolazione di partenza. Il compito di un'organizzazione esterna, che revisiona un processo di riconvalida utenze, è quello di verificare che gli utenti dichiarati non più idonei all'accesso siano stati correttamente estromessi dal sistema in questione.

Anche durante il processo di riconvalida delle utenze è inevitabile non affrontare criticità. Questi controlli in particolare trattano informazioni altamente sensibili come login ID, password, ruoli e privilegi, motivo per cui sono soggetti a un elevato tasso di rischio. Si individuano di seguito i principali rischi legati alla gestione delle impostazioni di sicurezza e dei diritti d'accesso:

- Gestione delle impostazioni di sicurezza:
    - Le impostazioni di sicurezza principali, comprese le password, possono non essere appropriate per limitare l'accesso ai soli utenti previsti;
    - Le impostazioni possono essere settate o modificate su valori non autorizzati, intenzionalmente o meno, e difficilmente possono essere rilevate e corrette in quanto si celano tra tutti gli altri dati.

- Gestione dei diritti di accesso:
    - Le richieste di accesso degli utenti IT e aziendali ai componenti rilevanti dell'ambiente IT possono essere effettivamente soddisfatte ma non appropriate;
    - L'accesso concesso ai componenti dell'ambiente IT può non corrispondere all'accesso approvato (se non si verifica alcuna approvazione, il rischio è che l'accesso concesso non corrisponda all'accesso richiesto);
    - I diritti di accesso possono non essere revocati tempestivamente;
    - Rischio di inadeguatezza nel tempo in quanto i diritti di accesso possono modificarsi con il passare del tempo.

Si possono identificare ulteriori rischi informatici, legati alla concessione e alla cessazione dell'accesso, che in genere riguardano l'uso dei ruoli per stabilire l'eventuale rimozione dell'accesso. I ruoli rappresentano diritti di accesso specifici. Quando i diritti di accesso sono rappresentati in modo inappropriato o vengono assegnati più ruoli a un utente, i ruoli assegnati possono conferire a tale utente diritti di accesso che violano la segregazione dei compiti previsti, sia per gli utenti aziendali, con accesso alle transazioni, sia per il personale IT.

Nei processi di gestione degli accessi possono essere utilizzati software di gestione delle identità e degli accessi. Quando si utilizzano altri software, esistono rischi legati al fatto che questi ultimi non funzionino come previsto, che siano configurati in modo inappropriato e/o che le configurazioni appropriate non vengano mantenute.

2.6.2 PROGETTAZIONE E TEST ITGC DI RICONVALIDA DELL'UTENTE

Il controllo di User Revalidation è un controllo di tipo detective, ovvero progettato per trovare errori o problemi in un momento successivo a quello in cui avviene la transazione (in questo caso l'approvazione o l'eliminazione dell'utente). La riconvalida delle utenze, infatti, rappresenta un check di controllo ulteriore al processo in cui vengono aggiornati gli accessi; l'obiettivo è quello di verificare che siano stati effettivamente presi i provvedimenti richiesti e che lo sia stato fatto rispettando le tempistiche. Non è un compito del controllo di rivalidazione utenze quello di valutare la bontà o meno delle decisioni prese dai validatori.

I controlli detective avvengono dopo quelli preventivi, e sono essenziali affinché possa essere dimostrato che i precedenti controlli, di user provisioning e user termination, siano andati a buon fine.

Lo scopo del controllo è intercettare i potenziali cambi mansione non accompagnati da un cambio ruolo/grant o le potenziali dimissioni non accompagnate da un blocco/dismissione sul sistema target.

Le fasi che deve seguire un processo di rivalidazione interno possono essere ripercorse attraverso i seguenti step:

1. Il Dipartimento IT, dopo aver effettuato l'estrazione utenze (con il dettaglio dei ruoli associati) dal sistema target e applicato i filtri necessari, condivide la lista con i vari validatori tramite e-mail/sistema di ticketing/sharepoint. Se è presente un Tool preposto all'attività, a seconda delle casistiche, il Dipartimento IT può effettuare l'upload delle liste utenze da validare (con il dettaglio dei ruoli associati) sul Tool o tramite integrazione. Viene effettuato quindi un upload automatico dal sistema target;

2. I validatori rispondono per le utenze di loro competenza tramite e-mail/sistema di ticketing/sharepoint/Tool;

3. Il Dipartimento IT procede con l'implementazione delle modifiche richieste. In presenza di un Tool integrato con il sistema target, l'implementazione delle modifiche può avvenire automaticamente.

È fondamentale che il Dipartimento IT sia a conoscenza dell'associazione Utenza-Rivalidatore per tutte gli users da rivalidare. Questa associazione può essere definita su una lista validata periodicamente o su un sistema HR. In presenza di un Tool, l'associazione può essere definita automaticamente all'interno dello stesso (in presenza di integrazioni con il sistema target e un sistema HR) o viene inserita manualmente dal Dipartimento IT.[34]

Interviene quindi il controllo di user revalidation, con una frequenza annuale o al più semestrale, che ha il compito di giudicare il processo svolto dal dipartimento IT. Il controllo è costituito dalla verifica dei seguenti tre requisiti fondamentali:

1. **Completezza della rivalidazione**

La completezza della rivalidazione implica che tutte le utenze, con i ruoli ad esse associati, siano verificate; cioè che le utenze che dovevano entrare in rivalidazione, abbiano effettivamente fatto parte del processo.

Per questo requisito si procede partendo dalla lista delle utenze entrate in rivalidazione. Questa lista si ottiene dalla società che ha effettuato la riconvalida ed è necessario che, in questa documentazione, siano indicati gli eventuali filtri applicati (es. esclusione delle user inattive, esclusione delle utenze di sistema senza possibilità di log-in, ecc…) successivamente all'estrazione dal sistema. È opportuno inoltre valutare l'appropriatezza dei dati stessi.

Quindi si verifica che queste liste siano conformi all'estrazione indipendente delle utenze da sistema, datata precedentemente all'inizio della rivalidazione, attraverso un'evidenza di C&A (completezza e accuratezza) e procedure di match tra

[34] Methodology weekly meeting Review delle utenze e dei profili Giugno 2020, EY

l'estrazione ottenuta e il set di utenze da validare, ovvero da inoltrare ai validatori assegnati a quelle utenze.

Maggiore sarà la differenza temporale tra la data di riferimento dell'estrazione e la data di inizio rivalidazione, maggiori saranno i "falsi positivi" individuati dal match (questo perché tra le due date possono essere avvenute creazioni utenze, modifiche utenze e terminazioni). È quindi ottimale ottenere l'estrazione indipendente in data più prossima possibile all'inizio della rivalidazione.

2. **Verifica dell'effettiva rivalidazione da parte dei reviewer**

Il secondo step di verifica è relativo ai ritorni dei validatori e all'effettiva implementazione delle eventuali modifiche richieste.

Per questo requisito si procede partendo dal listato dei ritorni dei validatori con il dettaglio delle conferme/modifiche per tutte le utenze entrate in rivalidazione. Viene quindi effettuato un match tra la lista precedentemente costruita, contenente le utenze da inviare ai validatori, e la lista con le risposte fornite dagli stessi.

Ai fini del soddisfacimento di questo requisito occorre verificare che, per ogni utenza, e per i ruoli ad esse associati, sia stato effettivamente fornito un feedback, positivo o negativo, da parte dei validatori.

Occorre inoltre verificare che non ci siano stati casi di auto-validazioni; questo è facilmente verificabile dall'associazione user-validatore ottenuta nello step precedente. Per questa verifica ci possono essere casistiche particolari poiché, data la struttura piramidale delle aziende, possono essere intercettate posizioni apicali non caratterizzate da un validatore terzo.

3. **Verifica dell'effettiva eliminazione delle utenze dichiarate da disabilitare**

A conclusione del controllo è necessario verificare che le modifiche indicate dai validatori siano state correttamente apportate. Per questo requisito occorre

confrontare la lista contenente i feedback forniti dai validatori con un'estrazione da sistema successiva al processo di rivalidazione. Anche in questo caso viene verificato che questa lista sia conforme all'estrazione indipendente delle utenze da sistema, datata successivamente la fine della rivalidazione, attraverso un'evidenza di C&A.

In caso di mancate risposte da parte dei validatori è applicata la regola di silenzio diniego; deve essere verificato che, a tutte le utenze per cui non è stato associato alcun feedback, sia stato negato l'accesso o bloccate.

Anche in questa condizione, maggiore sarà la differenza temporale tra la data di riferimento dell'estrazione e la data di fine rivalidazione, maggiori saranno i falsi positivi individuati dal match. È quindi ottimale ottenere l'estrazione indipendente, in data più prossima alla fine della rivalidazione.

La maggior parte di queste procedure vengono svolte attraverso funzioni di Microsoft Excel che permettono di confrontare più fogli contenenti le varie liste, permettendo così un confronto più rapido rispetto a un check puntuale, ma al contempo accurato.

Essendo la User Revalidation, come detto in precedenza, un controllo successivo a quelli di User Provisioning e User Termination, tale monitoraggio idealmente non dovrebbe individuare implementazioni alla fine del ciclo.

Poiché, nel concreto, sono presenti casistiche di richiesta/implementazione di modifiche (es. in seguito a migrazioni applicative, dovute a scostamenti dai processi di Provisioning/Termination, ecc…), potrebbe essere d'aiuto effettuare un Risk Assessment sulle principali criticità di seguito elencate:

- Identificazione dei ruoli associati alle utenze impattate da una modifica e il periodo di riferimento di tali ruoli (dalla data in cui avrebbero dovuto essere modificati alla data effettiva di modifica al termine della rivalidazione);
- Identificazione delle attività effettuate dalle utenze con i ruoli identificati nel periodo di riferimento;
- Ottenimento delle autorizzazioni per tali attività e valutazione dell'impatto delle stesse.

Occorre comunque valutare se, precedentemente, sono già stati effettuati controlli, che affrontino il tema del rischio esaustivamente e che rendono pertanto il Risk Assessment ridondante.

2.7 VALUTAZIONI FINALI SUI PROCESSI IT

Una volta analizzati approfonditamente i principali processi IT intrapresi da una società di revisione contabile, è possibile visualizzare più chiaramente la struttura che regge tutto il meccanismo di revisione. È quindi possibile comprendere la validità dei controlli, attraverso la valutazione del progetto e dell'implementazione risultante come efficace o inefficace, per ogni ITGC identificato.

Una valutazione sull'efficacia del progetto, dell'implementazione dei vari ITGC e di tutte le procedure informatiche eseguite, può essere utilizzata per stabilire se ogni processo informatico pertinente affronta adeguatamente i rischi informatici in quel processo.

Le valutazioni sui processi IT sono affrontate per quattro possibili scenari:

Effective → se per gli ITGC legati al processo IT che hanno funzionato efficacemente per tutto il periodo di revisione.

Reliable → se per almeno un rischio inerente al processo informatico sono state utilizzate procedure sostanziali ai fini di ottenere prove sufficienti a dimostrare che il rischio informatico non si sia verificato.

Ineffective → Se non esistono sufficienti ITGC efficaci, e gli ITGC compensativi o le procedure sostanziali IT non sono in grado di fornire prove sufficienti per affrontare i rischi.

Not tested → Se i rischi IT non sono stati affrontati testando gli ITGC.

Un'altra tipologia di valutazioni è rappresentata dalla "aggregate IT". Queste rappresentano l'effetto che le valutazioni hanno sui processi IT utilizzati, sui relativi controlli applicativi e sugli ITDM testati. Si suddividono in:

FS & ICFR Support → per cui tutti i processi IT di supporto sono stati valutati come efficaci

FS Only Support → almeno uno dei processi IT di supporto è stato valutato come Affidabile e i restanti processi IT di supporto sono stati valutati come Efficaci

Not Support → uno o più processi IT di supporto sono stati valutati come inefficaci o non testati.

La fase di valutazione finale è un punto chiave per una corretta revisione; un controllo ulteriore per verificare e riassumere eventuali problematiche riscontrate durante le fasi precedenti, e poter garantire un audit che presenti rischi e criticità minime.

CAPITOLO III

CASO STUDIO NEL CONTESTO AZIENDALE

3.1 INTRODUZIONE

Il caso studio riportato a conclusione del lavoro di tesi, tratta l'applicazione di una procedura in ambito Audit IT durante il tirocinio curriculare, presso la società EY Advisory S.p.A., all'interno del team del dominio Technology Risk.

Lo stage condotto in azienda ha consentito di sfruttare modelli di controllo in ambito progettuale per conto di società multinazionali, con particolare focus su attività di gestione del rischio IT, assicurando ai clienti un supporto idoneo per la loro Governance e Compliance IT.

I ruoli e le responsabilità di un auditor interno hanno rappresentato riferimenti indispensabili per instaurare un rapporto fiduciale con i clienti, il cui incarico è innegabilmente importante nell'ambito della consulenza. Si definisce di seguito l'iter che un processo di audit deve intraprendere per una corretta revisione di bilancio.

La prima fase consiste nella individuazione degli obiettivi dell'audit IT, specificatamente finalizzati alla revisione dei sistemi informativi a supporto della revisione contabile. Una volta acquisito il cliente viene stabilito un progetto ad-hoc che si adatti alle particolari esigenze della società. Uno strumento utilizzato in questa fase è la EY Global Audit Methodology (EY GAM), che fornisce un quadro globale per l'applicazione di un processo coerente a tutti gli audit. La metodologia EY GAM si applica a tutte le revisioni, ma è personalizzata per rispondere alle caratteristiche del tipo di entità sottoposta a revisione e ai principi di revisione applicabili alla revisione.[35] L'obiettivo è ricercare caratteristiche simili tra i progetti affrontati in precedenza, in modo da standardizzare il processo ed essere in grado di affrontare situazioni nuove sfruttando l'esperienza pregressa. Per completare la

[35] EY Atlas – "...provides a global framework for applying a consistent thought process to all audits. EY GAM applies to all audits but is customized to address the characteristics of the type of entity under audit and the auditing standards applicable to the audit."

pianificazione iniziale, si determina l'ambito dei servizi incontrando i responsabili della governance e/o della gestione, in modo da conoscere le loro aspettative e i loro requisiti di servizio. Si crea quindi un team, che comprende, a seconda dei casi, professionisti con conoscenze specifiche, come fiscali o informatiche, e specialisti, che si occupano di valutazioni.

In questa fase si effettua un'analisi sui rischi, valutando la probabilità di inesattezze significative. Studiando la natura di ciascuna attività e del relativo ambiente (in termini di bilancio) si stabiliscono i rischi che l'entità deve affrontare. È possibile così individuare le voci di conto e le informazioni significative.

Si effettua quindi una pianificazione strategica sviluppando un audit plan, progettando una adeguata risposta ai rischi di inesattezze significative precedentemente identificate. Si identificano natura, tempistiche ed estensione dei test sui controlli, strutturando le procedure sostanziali in risposta ai rischi valutati. Sono inoltre eseguite procedure revisionali specifiche per aree particolari, come le operazioni riguardanti parti correlate, leggi e regolamenti d'interesse per la società in questione. Questa parte dell'audit rappresenta le fondamenta dello stesso, e si basa su riferimenti Normativi, Framework e Standard precedentemente nel Capitolo II. Tra i principali si individuano: Sarbanes-Oxley Act (SOX), L.262/05, D.Lgs. n. 231/01, General Data Protection Regulation (GDPR), COBIT19, ITIL, ISAE 3402, ISO27001, ISO22301, ISA315.

Redigendo i primi documenti sulla comprensione degli SCOT, dei processi di informativa e dei controlli significativi, ha inizio la fase di revisione che prosegue attraverso procedure sostanziali e specifiche. Gli output prodotti sono in continua valutazione, in modo da rivalutare costantemente i rischi nel corso della revisione e determinare, eventualmente, una modifica della strategia di revisione.

La fase finale di un audit è rappresentata dal completamento della revisione, con successiva comunicazione dei risultati e delle questioni significative ai responsabili della governance e/o alla direzione. Avviene quindi una valutazione finale atta a dichiarare se ci sono elementi probatori, appropriati e a sufficienza, per fornire, con ragionevole certezza, un responso positivo sul bilancio. Esso, nel suo complesso, non deve contenere errori significativi, dovuti a frodi o errori.

In questo ambiente giovane e dinamico, esperti Senior e Manager illustrano il funzionamento dei vari programmi ed i tool da utilizzare all'interno dall'organizzazione, in modo da permettere la partecipazione, all'interno del team progettuale, anche di risorse con poca esperienza. Un esempio di tool utilizzato per condividere l'avanzamento del progetto in tempo reale con i clienti e monitorare le scadenze di ciascuna commessa, è EY Canvas[36], su cui vengono caricati tutti i documenti di revisione prodotti dallo staff interno.

Per un corretto e accurato svolgimento delle analisi, è usato il pacchetto Office 365, in particolare il programma Microsoft Excel. Non meno importante è la conoscenza degli standards, di cui occorre verificare il corretto adempimento.

Il valore da dare al cliente e le relative modalità con cui interagire, assumono un ruolo di primaria importanza durante il percorso di auditing. Col tempo e il supporto del team, un ulteriore elemento rilevante è l'interfacciarsi con le varie aziende, cui EY fornisce consulenza, tramite e-mail ed incontri. Un ulteriore strumento di sviluppo è rappresentato dai corsi di aggiornamento previsti dall'azienda, che permettono di migliorare ed affinare sempre più tecniche e monitorare i feed back, verificando, anche attraverso un contesto più generale, la visione strategica dell'organizzazione.

[36] https://eycanvas.ey.net/

3.2 ATTIVITA' DI USER REVALIDATION

Il particolare controllo trattato in questo caso studio viene svolto con frequenza annuale iniziando con la fase di understanding, fino ad arrivare all'esito finale in concomitanza con la chiusura dell'anno fiscale. L'obiettivo è quello di verificare che le azioni intraprese nei confronti delle utenze che popolano l'applicativo, siano allineate con le decisioni indicate dai soggetti autorizzati.

La fase iniziale prevede un colloquio con i referenti della società cliente, in cui vengono esplicitate le funzionalità dell'applicativo su cui si eseguirà il test. Questi meeting rappresentano la fase più delicata ai fini della comprensione dell'applicativo; infatti, attraverso l'esperienza, un auditor deve essere in grado di riconoscere i rischi descritti nel capitolo 2.6.1, cui può essere soggetto il software. L'applicativo può essere gestito sia tramite il supporto di tool automatizzati, sia manualmente, ovvero tramite confronti personali inter-aziendali. Il controllo da eseguire cambia a seconda delle caratteristiche di gestione dello stesso; pertanto saranno trattati due esempi relativi ai due casi di rivalidazione.

La seconda fase è costituita dal raccogliere e catalogare la documentazione prodotta dal cliente, la quale deve rispettare i requisiti della Legge Sarbanes Oxley descritti precedentemente nel capitolo 1.4.
Si riportano di seguito i requisiti di completezza e accuratezza richiesti dalla Normativa SOX per quanto riguarda la documentazione che deve essere fornita[37]:

- Print Screen: è richiesto il formato a schermo intero. Le istruzioni necessarie a garantire la completezza e accuratezza dei dati prevedono:
    a. di non ritagliare parzialmente l'immagine, in quanto è necessario catturare l'intera schermata;

[37] Tratto da una richiesta di documentazione per una società sottostante alla Normativa SOX.

b. che lo screenshot riporti la data, l'ora e il numero di record estratti; nel caso in cui i record/l'immagine risultano estesi su più parti, è necessario accertarsi che l'ultimo record della prima pagina sia visibile sull'immagine successiva;
c. che, nel caso in cui non sia possibile ottenere il numero di record estratti, sia fornita l'evidenza dei primi e degli ultimi record, oppure la dimensione del file in byte.

- Popolazione: la popolazione deve essere verificabile. E' necessario quindi fornire le query utilizzate per generare Report Standard. Qualora non fosse possibile, è necessario fornire degli screenshot con l'evidenza dell'esecuzione della query (in formato images, word, excel) e gli eventuali filtri applicati.

La fase finale rappresenta il controllo vero e proprio, in cui, attraverso la documentazione ottenuta dai clienti, vengono effettuate le verifiche sul corretto adempimento della Legge.
Il caso studio tratterà come soggetto, una società del settore dell'automotive, quotata sul mercato americano e che pertanto deve rispettare i requisiti richiesti dalla SOX in ambito Information Security. Questa azienda sarà indicata come la "Società X". Le informazioni riportate di seguito, volte ai fini della comprensione del controllo, saranno parzialmente oscurate per tutelare le informazioni private del cliente.
Come già esposto nel capitolo II, si illustra un ITGC in particolare, quello di user revalidation o riconvalida delle utenze. Questo test deve essere effettuato successivamente all'esecuzione del controllo da parte dell'azienda in questione, nel rispetto della normativa SOX, con l'obiettivo di valutarne "bontà" e tempistiche dei provvedimenti presi per la popolazione trattata su un dato applicativo.
Il controllo di riconvalida delle utenze è un ITGC che si colloca all'interno del processo di Manage Access, che presidia la parte relativa alla gestione delle utenze per la Società X.

In particolare si occupa:
della parte relativa a creazione e modifica delle autorizzazioni conferite a un'utenza; del rispetto delle direttive riguardanti la policy per gli utenti che possono farne richiesta; del trattamento delle utenze che durante il corso dell'anno vengono disattivate o private di alcuni accessi e parametri di autenticazione.
Ciascun applicativo può essere trattato seguendo diversi metodi di rivalidazione a seconda della struttura dello stesso. Elementi chiave per la scelta del metodo sono la quantità di dati gestiti dall'applicativo e il workflow che viene seguito dal processo. Più un'applicativo è semplice e con poche informazioni più sarà conveniente utilizzare metodi di rivalidazione non automatizzati, viceversa, più risulta complesso e con alti volumi di dati, più sarà vantaggioso utilizzare dei tool computerizzati.

La Società X ha sfruttato due metodi di rivalidazione:

1. Tramite e-mail, la popolazione di utenze viene valutata manualmente, ovvero tramite un processo di scambio di e-mail tra Control Owner, responsabile dell'esecuzione del controllo di rivalidazione e rivalidatori (vedi Figura 3.1);

2. Tramite tool automatizzato, un processo che invece utilizza un tool automatico per la valutazione delle utenze (Vedi Figura 3.2).

Entrambi i processi partono da una lista di utenze attive sull'applicativo oggetto di rivalidazione., in cui sono presenti tutte le utenze che fanno parte dell'organizzazione e terminano il processo attraverso una seconda estrazione post-rivalidazione.

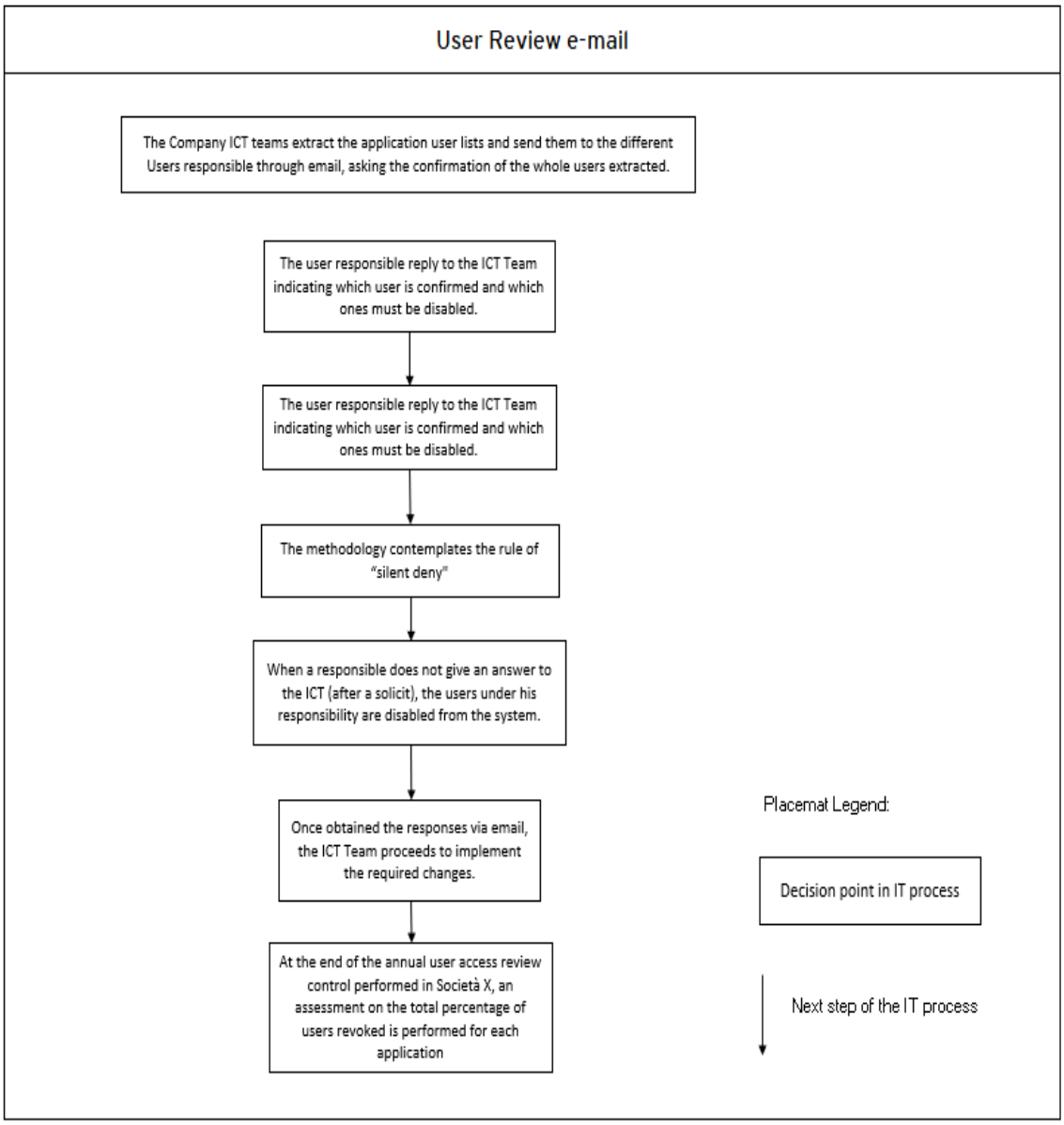


Figura 3.1: Placemat tratto da un test di rivalidazione tramite e-mail effettuato per la Società X

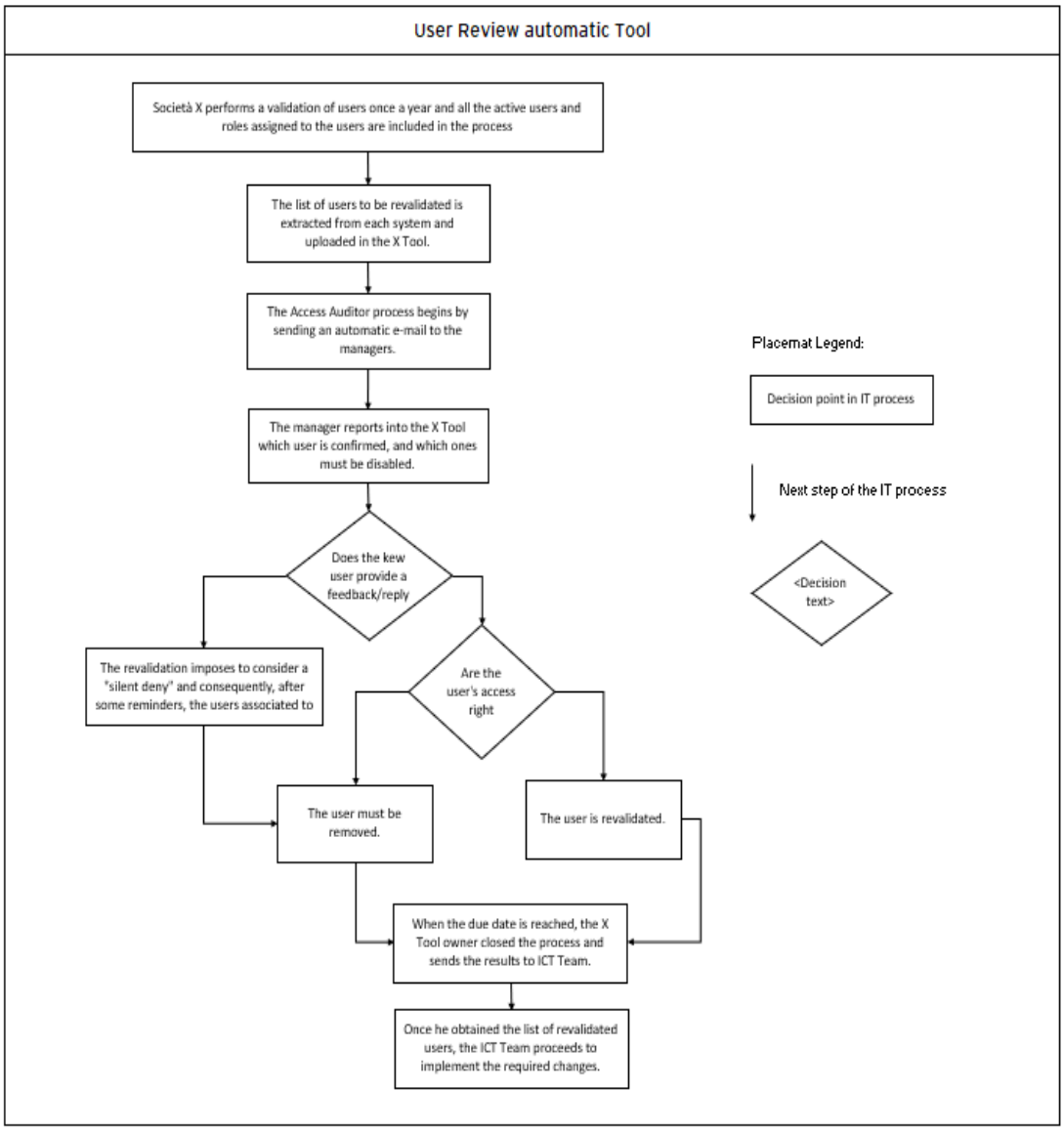


Figura 3.2: Placemat tratto da un controllo di rivalidazione tramite il Tool X effettuato per la Società X

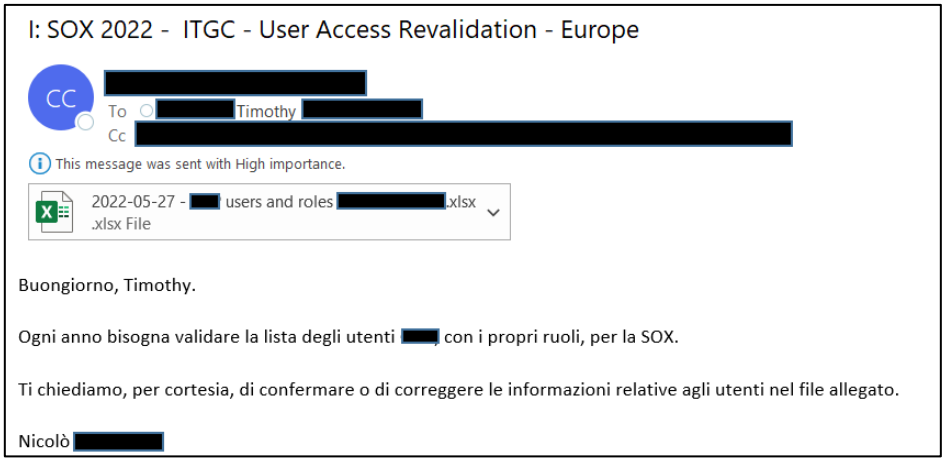
Indipendentemente dal tipo di rivalidazione effettuata, l'auditor IT verifica il soffisfacimento dei seguenti attributi di controllo:

1. the Company extracted the application user list with related completeness;
2. the Company defined for each user or profile a specific reviewer;
3. verification of the percentage of 'denied' in relation to the population as a whole;
4. each reviewer performed the revalidation and that in case of missing reply the Company applied the silent-deny rule.[38]

[38] Requisiti tratti da un controllo generico effettuato da EY.

3.3 RIVALIDAZIONE TRAMITE E-MAIL

La lista di utenze aventi accesso all'applicativo Y della Società X, con le informazioni riguardanti i ruoli ad essi associati viene estratta da sistema e inviata tramite e-mail al rivalidatore designato per la valutazione di queste utenze. Nel caso preso in esame, come riportato nella Figura 3.1, Timothy rappresenta il soggetto che si occupa di questa fase del processo, ovvero il rivalidatore.



I: SOX 2022 - ITGC - User Access Revalidation - Europe

CC [redacted]

To [redacted] Timothy [redacted]

Cc [redacted]

This message was sent with High importance.

2022-05-27 - [redacted] users and roles [redacted].xlsx
.xlsx File

Buongiorno, Timothy.

Ogni anno bisogna validare la lista degli utenti [redacted] con i propri ruoli, per la SOX.

Ti chiediamo, per cortesia, di confermare o di correggere le informazioni relative agli utenti nel file allegato.

Nicolò [redacted]

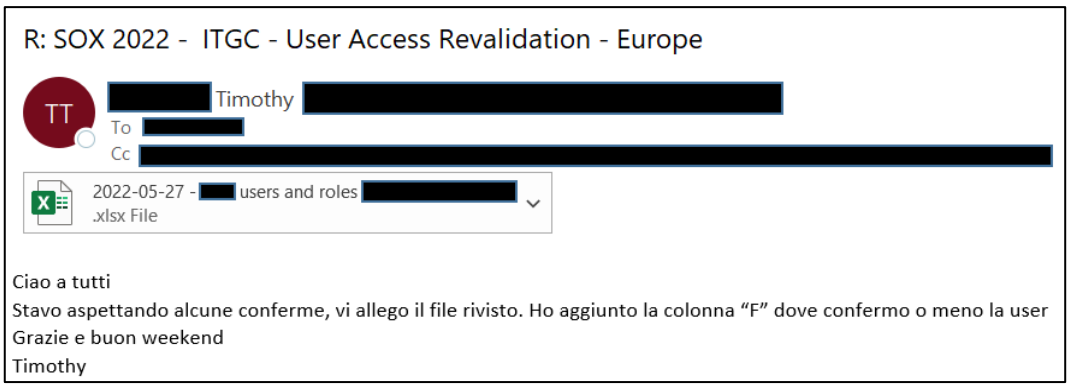
Figura 3.1: e-mail contenente le utenze da revisionare

Nelle colonne del file riportato in Figura 3.2 sono contenute le informazioni riguardanti le n utenze, tra le più significative vengono individuate la data di creazione, l'ultimo accesso e lo stato attuale dell'utente (attivo – non attivo).

	A	B	C	D	E	F
1	DATE AND TIME OF EXPORT	USER LOGIN	USER NAME	CREATION DATE	LAST ACCESS	ACTIVE / NOT ACTIVE
2	2022/05/27 17:08:02	[redacted]	Adam [redacted]	09/12/2019 00:00:00	05/25/2022 00:00:00	YES
3	2022/05/27 17:08:02		[redacted]Marco	07/10/2017 00:00:00	12/21/2021 00:00:00	YES
4	2022/05/27 17:08:02		[redacted]Christopher	02/03/2022 00:00:00	05/20/2022 00:00:00	YES
5	2022/05/27 17:08:02		Albrecht [redacted]	04/28/2015 00:00:00	03/04/2021 00:00:00	YES
6	2022/05/27 17:08:02		Alex [redacted]	06/28/2021 00:00:00	07/12/2021 00:00:00	YES
7	2022/05/27 17:08:02		Andrew [redacted]	09/20/2021 00:00:00	09/20/2021 00:00:00	YES
8	2022/05/27 17:08:02		[redacted]Nicolo		05/27/2022 00:00:00	YES
9	2022/05/27 17:08:02		[redacted]		03/09/2022 00:00:00	YES
10	2022/05/27 17:08:02			09/12/2019 00:00:00	05/19/2022 00:00:00	YES
11	2022/05/27 17:08:02			04/03/2018 00:00:00	08/18/2020 00:00:00	YES
12	2022/05/27 17:08:02			03/11/2021 00:00:00	02/25/2022 00:00:00	YES
13	2022/05/27 17:08:02			11/28/2017 00:00:00	02/22/2019 00:00:00	YES
14	2022/05/27 17:08:02			06/03/2019 00:00:00	06/03/2019 00:00:00	YES
15	2022/05/27 17:08:02			11/07/2017 00:00:00	02/21/2022 00:00:00	YES
16	2022/05/27 17:08:02			10/19/2018 00:00:00		YES
17	2022/05/27 17:08:02				02/14/2020 00:00:00	YES
18	2022/05/27 17:08:02				08/15/2021 00:00:00	YES
19	2022/05/27 17:08:02			10/07/2020 00:00:00	05/27/2022 00:00:00	YES
20	2022/05/27 17:08:02			04/16/2015 00:00:00		YES
21	2022/05/27 17:08:02			10/19/2018 00:00:00	09/10/2020 00:00:00	YES
22	2022/05/27 17:08:02			01/20/2021 00:00:00	05/04/2022 00:00:00	YES
23	2022/05/27 17:08:02			01/20/2021 00:00:00	10/26/2021 00:00:00	YES
24	2022/05/27 17:08:02			02/12/2018 00:00:00	06/14/2019 00:00:00	YES
25	2022/05/27 17:08:02			07/24/2019 00:00:00	05/26/2022 00:00:00	YES

Figura 3.2: lista utenze pre-rivalidazione

A questo punto il rivalidatore indica il proprio feedback riguardo le utenze, solitamente aggiungendo una colonna al file di partenza in cui dichiara il suo responso (es. Da rimuovere – Confermato) allegando nuovamente il file con le decisioni prese riguardo ciascuna utenza (Figura 3.3).


R: SOX 2022 - ITGC - User Access Revalidation - Europe

TT [redacted] Timothy [redacted]

To [redacted]

Cc [redacted]

2022-05-27 - [redacted] users and roles [redacted]
.xlsx File

Ciao a tutti
Stavo aspettando alcune conferme, vi allego il file rivisto. Ho aggiunto la colonna "F" dove confermo o meno la user
Grazie e buon weekend
Timothy

Figura 3.2.3: e-mail contenente il responso del rivalidatore

Nella Figura 3.4 Timothy ha elaborato la lista aggiungendo l'azione richiesta per ciascun utente (vedi colonna G 'ACTION'). Nell'esempio preso in considerazione conferma la maggior parte delle utenze, mentre chiede la rimozione dell'utente Albrecht (vedi riga 5), dato che sarà utilizzato in seguito come campione per la verifica del corretto processo di rivalidazione.

	A	B	C	D	E	F	G
1	DATE AND TIME OF EXPORT	USER LOGIN	USER NAME	CREATION DATE	LAST ACCESS	ACTIVE / NOT ACTIVE	ACTION
2	2022/05/27 17:08:02	[redacted]	Adam [redacted]	09/12/2019 00:00:00	05/25/2022 00:00:00	YES	OK
3	2022/05/27 17:08:02		[redacted] Marco	07/10/2017 00:00:00	12/21/2021 00:00:00	YES	OK
4	2022/05/27 17:08:02		[redacted]Christopher	02/03/2022 00:00:00	05/20/2022 00:00:00	YES	OK
5	2022/05/27 17:08:02		Albrecht [redacted]	04/28/2015 00:00:00	03/04/2021 00:00:00	YES	Remove
6	2022/05/27 17:08:02		Alex [redacted]	06/28/2021 00:00:00	07/12/2021 00:00:00	YES	OK
7	2022/05/27 17:08:02		Andrew [redacted]	09/20/2021 00:00:00	09/20/2021 00:00:00	YES	OK
8	2022/05/27 17:08:02		[redacted] Nicolo		05/27/2022 00:00:00	YES	OK
9	2022/05/27 17:08:02		[redacted]		03/09/2022 00:00:00	YES	OK
10	2022/05/27 17:08:02			09/12/2019 00:00:00	05/19/2022 00:00:00	YES	OK
11	2022/05/27 17:08:02			04/03/2018 00:00:00	08/18/2020 00:00:00	YES	OK
12	2022/05/27 17:08:02			03/11/2021 00:00:00	02/25/2022 00:00:00	YES	OK
13	2022/05/27 17:08:02			11/28/2017 00:00:00	02/22/2019 00:00:00	YES	OK
14	2022/05/27 17:08:02			06/03/2019 00:00:00	06/03/2019 00:00:00	YES	OK
15	2022/05/27 17:08:02			11/07/2017 00:00:00	02/21/2022 00:00:00	YES	OK
16	2022/05/27 17:08:02			10/19/2018 00:00:00		YES	OK
17	2022/05/27 17:08:02				02/14/2020 00:00:00	YES	OK
18	2022/05/27 17:08:02				08/15/2021 00:00:00	YES	OK
19	2022/05/27 17:08:02			10/07/2020 00:00:00	05/27/2022 00:00:00	YES	OK
20	2022/05/27 17:08:02			04/16/2015 00:00:00		YES	OK
21	2022/05/27 17:08:02			10/19/2018 00:00:00	09/10/2020 00:00:00	YES	Remove
22	2022/05/27 17:08:02			01/20/2021 00:00:00	05/04/2022 00:00:00	YES	OK
23	2022/05/27 17:08:02			01/20/2021 00:00:00	10/26/2021 00:00:00	YES	OK
24	2022/05/27 17:08:02			02/12/2018 00:00:00	06/14/2019 00:00:00	YES	OK
25	2022/05/27 17:08:02			07/24/2019 00:00:00	05/26/2022 00:00:00	YES	OK

Figura 3.4: lista utenze con feedback del rivalidatore

La Società X ha il compito di intraprendere le azioni richieste dal rivalidatore: rimuovendo l'accesso agli utenti per cui è stata richiesta l'eliminazione; modificando le autorizzazioni degli utenti per cui è stato richiesto un cambio di ruolo (limitazioni o ampliamenti); confermando i precedenti requisiti delle utenze per cui non è stata indicata alcuna restrizione.

In caso di mancata risposta da parte di un rivalidatore viene applicata la regola del silenzio diniego, ovvero la rimozione delle credenziali di accesso all'applicativo per quell'utenza.

Termina così il processo di rivalidazione tramite e-mail.

Successivamente, tramite una seconda estrazione (Figura 3.5), occorrerà verificare la corretta eliminazione delle utenze per cui le autorizzazioni sono state dichiarate da revocare.

	A	B	C	D	E	F
1	DATE AND TIME OF EXPORT	USER LOGIN	USER NAME	CREATION DATE	LAST ACCESS	ACTIVE / NOT ACTIVE
2	2022/07/04 17:25:45	[redacted]	Adam [redacted]	12/09/2019	08/06/2022	YES
3	2022/07/04 17:25:45		[redacted] Marco	10/07/2017	21/12/2021	YES
4	2022/07/04 17:25:45		[redacted]Christopher	03/02/2022	28/06/2022	YES
5	2022/07/04 17:25:45		Alex [redacted]	28/06/2021	12/07/2021	YES
6	2022/07/04 17:25:45		Andrew [redacted]	20/09/2021	20/09/2021	YES
7	2022/07/04 17:25:45		Antonietti [redacted]		16/06/2022	YES
8	2022/07/04 17:25:45		[redacted] Dan		09/03/2022	YES
9	2022/07/04 17:25:45		Bartosz [redacted]	12/09/2019	30/06/2022	YES
10	2022/07/04 17:25:45		[redacted]	03/04/2018	18/08/2020	YES
11	2022/07/04 17:25:45			11/03/2021	25/02/2022	YES
12	2022/07/04 17:25:45			28/11/2017	22/02/2019	YES
13	2022/07/04 17:25:45			03/06/2019	03/06/2019	YES
14	2022/07/04 17:25:45			07/11/2017	21/02/2022	YES
15	2022/07/04 17:25:45			19/10/2018		YES
16	2022/07/04 17:25:45				14/02/2020	YES
17	2022/07/04 17:25:45				15/08/2021	YES
18	2022/07/04 17:25:45			07/10/2020	04/07/2022	YES
19	2022/07/04 17:25:45			16/04/2015		YES
20	2022/07/04 17:25:45			20/01/2021	16/06/2022	YES
21	2022/07/04 17:25:45			20/01/2021	26/10/2021	YES
22	2022/07/04 17:25:45			12/02/2018	14/06/2019	YES
23	2022/07/04 17:25:45			24/07/2019	04/07/2022	YES
24	2022/07/04 17:25:45			17/11/2021	23/06/2022	YES
25	2022/07/04 17:25:45				06/09/2021	YES

Figura 3.5: lista utenze post-rivalidazione

Per una corretta revisione occorre prima di tutto verificare la completezza e l'accuratezza delle liste utilizzate durante il processo di rivalidazione. A questo scopo, la Società X, fornisce a EY le evidenze riguardanti l'estrazione della popolazione, rispettanti i requisiti della Normativa descritti precedentemente. In questo modo è verificabile la coerenza dei dati inviati al rivalidatore con quelli estratti: deve quindi essere prodotta la prima documentazione che evidenzi il fatto

che non siano state apportate modifiche alla lista di partenza e quindi che nessun dato possa essere stato perso durante questa transizione. La Figura 3.6 riproduce lo screenshot che evidenzia la fase di estrazione della lista utilizzata per il processo di rivalidazione in cui sono evidenziate in giallo le caratteristiche più importanti da verificare e cioè:

1. nominativi degli utenti;
2. numero di record presenti nella lista;
3. data e ora dell'estrazione.

Questi valori devono corrispondere a quelli presenti nel formato '.xlsx' visto precedentemente in Figura 3.2, ovvero la lista inviata all'approvatore durante la fase iniziale del processo di user revalidation. In questo modo può essere dimostrato il soddisfacimento del requisito 1 del controllo.

Analogamente, occorre verificare la coerenza dei dati dell'estrazione post-rivalidazione.

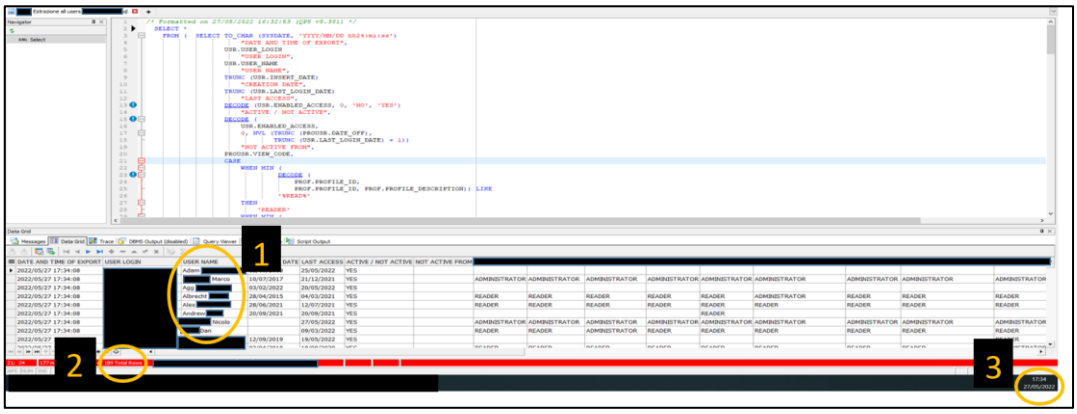


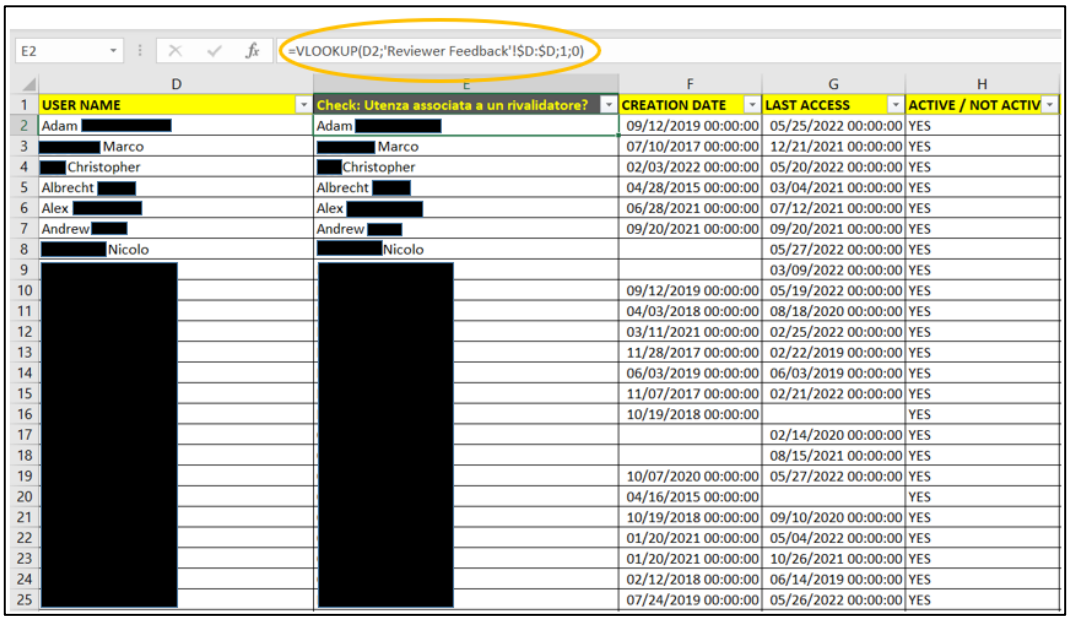
Figura 3.6: evidenza estrazione da sistema lista utenze pre-rivalidazione

Una volta verificato l'adempimento dei requisiti di completezza e accuratezza si può procedere con l'analisi vera e propria. Le liste estratte da sistema e quella con i feedback forniti dai rivalidatori vengono copiate in un unico file in cui, tramite apposite funzioni Excel, sono effettuati dei check incrociando i dati presenti in ognuna di esse. Per la verifica del secondo requisito del controllo, ovvero che ad ogni utenza sia stato correttamente associato un rivalidatore, vengono confrontate la lista estratta da sistema pre-rivalidazione con la lista contenente le azioni da

intraprendere per ciascuna utenza. L'obiettivo è quello di verificare che le stesse utenze siano presenti in entrambe le liste in modo da dimostrare che ogni utente è stato valutato. Nel caso preso in considerazione, essendo presente un unico rivalidatore, questa parte di controllo può essere considerata superata con un semplice incrocio. Come evidenziato in Figura 3.7, nella colonna E 'Check: Utenza associata a un rivaldatore?', viene effettuato un controllo tramite la funzione 'vlookup'. Essa può dare come output:

- il valore che si decide di cercare nel caso in cui questo sia presente nella lista in cui si effettua la ricerca (in questo caso sheet 'Reviewer Feedback', ovvero la lista contenente le risposte di Timothy);
- il valore #N/A nel caso in cui il nome non venisse trovato.

Se tutti i dati hanno una corrispondenza nella lista in cui si effettua la ricerca, e quindi nessun #N/A viene fornito come output da parte della funzione, allora il requisito può essere definito soddisfatto.



	D	E	F	G	H
1	USER NAME	Check: Utenza associata a un rivalidatore?	CREATION DATE	LAST ACCESS	ACTIVE / NOT ACTIV
2	Adam [redacted]	Adam [redacted]	09/12/2019 00:00:00	05/25/2022 00:00:00	YES
3	[redacted] Marco	[redacted] Marco	07/10/2017 00:00:00	12/21/2021 00:00:00	YES
4	[redacted]Christopher	[redacted]Christopher	02/03/2022 00:00:00	05/20/2022 00:00:00	YES
5	Albrecht [redacted]	Albrecht [redacted]	04/28/2015 00:00:00	03/04/2021 00:00:00	YES
6	Alex [redacted]	Alex [redacted]	06/28/2021 00:00:00	07/12/2021 00:00:00	YES
7	Andrew [redacted]	Andrew [redacted]	09/20/2021 00:00:00	09/20/2021 00:00:00	YES
8	[redacted] Nicolo	[redacted] Nicolo		05/27/2022 00:00:00	YES
9	[redacted]	[redacted]		03/09/2022 00:00:00	YES
10			09/12/2019 00:00:00	05/19/2022 00:00:00	YES
11			04/03/2018 00:00:00	08/18/2020 00:00:00	YES
12			03/11/2021 00:00:00	02/25/2022 00:00:00	YES
13			11/28/2017 00:00:00	02/22/2019 00:00:00	YES
14			06/03/2019 00:00:00	06/03/2019 00:00:00	YES
15			11/07/2017 00:00:00	02/21/2022 00:00:00	YES
16			10/19/2018 00:00:00		YES
17				02/14/2020 00:00:00	YES
18				08/15/2021 00:00:00	YES
19			10/07/2020 00:00:00	05/27/2022 00:00:00	YES
20			04/16/2015 00:00:00		YES
21			10/19/2018 00:00:00	09/10/2020 00:00:00	YES
22			01/20/2021 00:00:00	05/04/2022 00:00:00	YES
23			01/20/2021 00:00:00	10/26/2021 00:00:00	YES
24			02/12/2018 00:00:00	06/14/2019 00:00:00	YES
25			07/24/2019 00:00:00	05/26/2022 00:00:00	YES

Figura 3.7: check requisito 2 su lista pre-rivalidazione

Per la verifica del terzo requisito è necessario testare la corretta eliminazione delle utenze dichiarate da revocare, in quanto, se non fossero state effettivamente eliminate, rappresenterebbero un rischio elevato per l'applicativo.

In questa fase occorre iniziare dalla lista con le risposte fornite dall'approvatore, e il check va effettuato incrociando i dati con la lista estratta da sistema post-validazione. Pertanto, non si dovrà verificare la sola presenza dell'utenza all'interno della lista finale, ma lo stato in cui essa risulta. Per effettuare questo check viene utilizzata sempre la funzione 'vlookup' in modo da permettere controlli massivi che, se effettuati manualmente, richiederebbero troppo tempo. A scopo illustrativo viene effettuato un controllo manuale sul solo utente Albrecht indicato come da rimuovere (vedi Figura 3.4).

In Figura 3.8 sono evidenziati:

1. Il nome utente 'USER NAME' → Albrecht;
2. Lo stato 'ACTIVE NOT ACTIVE' → NO;
3. La data e l'ora di disattivazione 'NOT ACTIVE FROM' → 06/21/2022

	A	B	C	D	E	F	G
1	DATE AND TIME OF EXPORT	USER LOGIN	USER NAME	CREATION DAT	LAST ACCE	ACTIVE / NOT ACTIV	NOT ACTIVE FROM
2	2022/07/04 17:25:45	[redacted]	Aaron [redacted]	14/01/2019	14/01/2019	NO	11/16/2021 00:00:00
3	2022/07/04 17:25:45		Adam [redacted]	12/09/2019	08/06/2022	YES	
4	2022/07/04 17:25:45		[redacted] Marco	10/07/2017	21/12/2021	YES	
5	2022/07/04 17:25:45		[redacted]Christopher	03/02/2022	28/06/2022	YES	
6	2022/07/04 17:25:45		Albrecht	28/04/2015	04/03/2021	NO	06/21/2022 00:00:00
7	2022/07/04 17:25:45		Alex [redacted]	28/06/2021	12/07/2021	YES	
8	2022/07/04 17:25:45		Andrew [redacted]	20/09/2021	20/09/2021	YES	
9	2022/07/04 17:25:45		[redacted] Nicolo		16/06/2022	YES	
10	2022/07/04 17:25:45		[redacted]	06/04/2017	30/08/2017	NO	11/16/2021 00:00:00
11	2022/07/04 17:25:45			22/03/2021	24/08/2021	NO	11/08/2021 00:00:00
12	2022/07/04 17:25:45				09/03/2022	YES	
13	2022/07/04 17:25:45			12/09/2019	30/06/2022	YES	
14	2022/07/04 17:25:45				10/09/2015	NO	10/15/2018 00:00:00
15	2022/07/04 17:25:45			03/04/2018	18/08/2020	YES	
16	2022/07/04 17:25:45			11/03/2021	25/02/2022	YES	
17	2022/07/04 17:25:45			28/11/2017	22/02/2019	YES	
18	2022/07/04 17:25:45			07/11/2017	20/12/2018	NO	05/29/2019 00:00:00
19	2022/07/04 17:25:45			03/06/2019	03/06/2019	YES	
20	2022/07/04 17:25:45			07/11/2017	21/02/2022	YES	
21	2022/07/04 17:25:45			07/11/2017	07/11/2017	NO	05/29/2019 00:00:00
22	2022/07/04 17:25:45			19/10/2018		YES	
23	2022/07/04 17:25:45			29/08/2016	27/01/2017	NO	04/19/2017 00:00:00
24	2022/07/04 17:25:45				14/02/2020	YES	
25	2022/07/04 17:25:45			01/10/2018	04/07/2019	NO	10/24/2019 00:00:00

Figura 3.8: check requisito 3 su lista post-rivalidazione

Tutte le utenze dell'applicativo Y, dichiarate come da revocare o non revisionate, in corrispondenza della colonna 'ACTIVE/NOT ACTIVE' della lista estratta dopo il processo di rivalidazione, sono risultate essere effettivamente non più attive come nel caso di Albrecht. Poiché anche il terzo requisito è stato soddisfatto, il controllo sull'applicativo Y per la società X può essere dichiarato completato con esito positivo.

Il compito del revisore, una volta effettuata questa analisi tecnica, è quello di formalizzare il controllo all'interno di un'ulteriore carta che esplichi le modalità

con cui è arrivato ad affermare la bontà del processo. Il file dovrà contenere giustificazioni riguardanti i ragionamenti effettuati durante la fase di analisi, e gli allegati a cui si fa riferimento con evidenziate le parti chiave della revisione, suddividendole in funzione dei requisiti richiesti dal controllo. I vari file vengono quindi caricati all'interno del tool condivisi con la Società X e firmati dal revisore.

3.4 RIVALIDAZIONE TRAMITE TOOL

Il processo di rivalidazione delle utenze con un tool automatizzato, si differenzia rispetto al processo per e-mail nella parte in cui avviene la valutazione delle utenze. Pur rimanendo invariati gli attributi del controllo, la modalità operativa si differenzia dal processo di rivalidazione tramite e-mail. Il tool interviene ad un livello più basso del processo, in cui, per poter gestire più agevolmente ingenti flussi di dati, vengono sfruttate le potenzialità dell'automatismo, riducendo al minimo gli interventi manuali che richiederebbero moltissimo tempo e/o risorse.

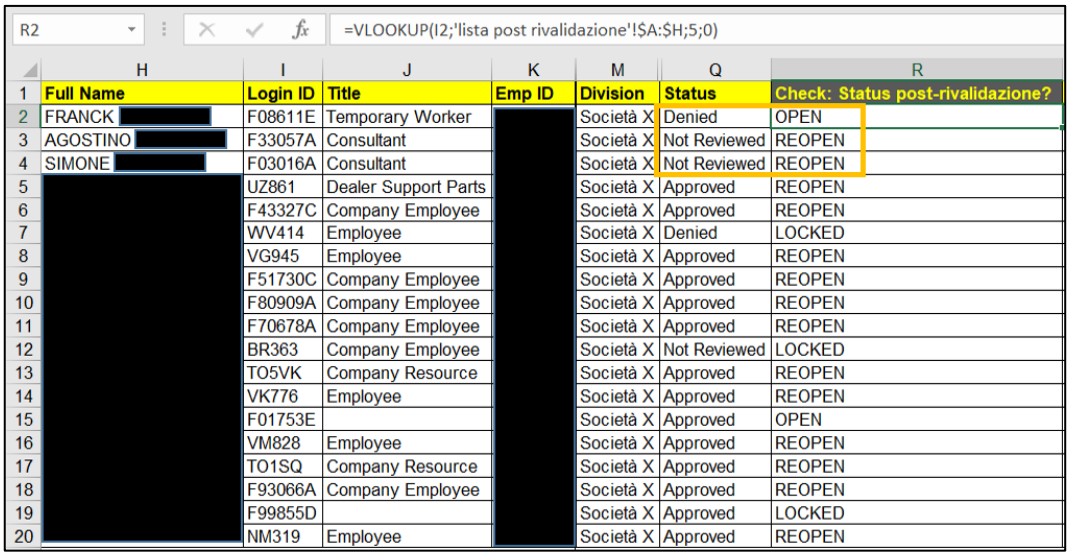
Le estrazioni delle liste da sistema e i relativi controlli di completezza e accuratezza e incroci con le liste contenenti i feedback, sono effettuati analogamente al caso visto in precedenza. Viene pertanto illustrata esclusivamente la parte finale del controllo per l'applicativo applicativo Z, sempre riguardante la Società X, per cui si sono verificati alcuni casi di errore. L'applicativo trattato è stato scelto appositamente per illustrare la fase di mitigazione da intraprendere nell'eventualità di incoerenze riscontrate durante l'analisi. Mentre l'applicativo Y non ha presentato alcuna eccezione, e il controllo su di esso dichiarato concluso con esito positivo in modo lineare, per l'applicativo Z, alcune utenze indicate come da revocare o 'Not Reviewed', sono state rilevate ancora attive nel controllo post-rivalidazione. È pertanto interessante approfondire le azioni che, con il team e la Società X, sono state intraprese al fine di mitigare il rischio presente su Z. Utilizzando le regole di applicazione incrociata, il tool in questione, aiuta a far rispettare la separazione dei ruoli in maniera automatica, fornendo come output un responso riguardo l'utenza presa in considerazione. Viene di seguito riportato (Figura 3.9) l'output che fornisce il tool, modificato a scopo illustrativo, in modo da mettere in evidenza le utenze per cui sono state riscontrate alcune discrepanze e le colonne più significative.

	H	I	J	K	M	Q	R
1	**Full Name**	**Login ID**	**Title**	**Emp ID**	**Division**	**Status**	**Reviewer**
2	FRANCK [redacted]	F08611E	Temporary Worker	[redacted]	Società X	Denied	[redacted]
3	AGOSTINO [redacted]	F33057A	Consultant		Società X	Not Reviewed	
4	SIMONE [redacted]	F03016A	Consultant		Società X	Not Reviewed	
5	[redacted]	UZ861	Dealer Support Parts		Società X	Approved	
6		F43327C	Company Employee		Società X	Approved	
7		WV414	Employee		Società X	Denied	
8		VG945	Employee		Società X	Approved	
9		F51730C	Company Employee		Società X	Approved	
10		F80909A	Company Employee		Società X	Approved	
11		F70678A	Company Employee		Società X	Approved	
12		BR363	Company Employee		Società X	Not Reviewed	
13		TO5VK	Company Resource		Società X	Approved	
14		VK776	Employee		Società X	Approved	
15		F01753E			Società X	Approved	
16		VM828	Employee		Società X	Approved	
17		TO1SQ	Company Resource		Società X	Approved	
18		F93066A	Company Employee		Società X	Approved	
19		F99855D			Società X	Approved	
20		NM319	Employee		Società X	Approved	

Figura 3.9: lista fornita come output dal tool automatico

Dopo aver verificato che in questa lista fossero presenti tutte le utenze attive sull'applicativo Z, e quindi che la rivalidazione fosse stata effettuata sulla totalità delle utenze, il compito del revisore è stato quello di verificare la corretta esecuzione delle azioni richieste nei confronti delle utenze.

Nel caso dell'applicativo in questione sono state rilevate diverse utenze dichiarate 'Denied' o prive di un approvatore, per cui quindi, era necessaria una revoca delle autorizzazioni d'accesso. Il check visibile nella colonna R della Figura 3.10 riporta lo stato in cui si trovavano le utenze corrispondenti al momento dell'estrazione post-rivalidazione. Questo check dimostra come, per le prime tre utenze, indicate come 'Denied' o 'Not reviewed', non è avvenuta alcuna chiusura, anzi hanno mantenuto l'accesso o sono state addirittura riaperte.



R2 =VLOOKUP(I2;'lista post rivalidazione'!$A:$H;5;0)

	H	I	J	K	M	Q	R
1	**Full Name**	**Login ID**	**Title**	**Emp ID**	**Division**	**Status**	**Check: Status post-rivalidazione?**
2	FRANCK [redacted]	F08611E	Temporary Worker	[redacted]	Società X	Denied	OPEN
3	AGOSTINO [redacted]	F33057A	Consultant		Società X	Not Reviewed	REOPEN
4	SIMONE [redacted]	F03016A	Consultant		Società X	Not Reviewed	REOPEN
5	[redacted]	UZ861	Dealer Support Parts		Società X	Approved	REOPEN
6		F43327C	Company Employee		Società X	Approved	REOPEN
7		WV414	Employee		Società X	Denied	LOCKED
8		VG945	Employee		Società X	Approved	REOPEN
9		F51730C	Company Employee		Società X	Approved	REOPEN
10		F80909A	Company Employee		Società X	Approved	REOPEN
11		F70678A	Company Employee		Società X	Approved	REOPEN
12		BR363	Company Employee		Società X	Not Reviewed	LOCKED
13		TO5VK	Company Resource		Società X	Approved	REOPEN
14		VK776	Employee		Società X	Approved	REOPEN
15		F01753E			Società X	Approved	OPEN
16		VM828	Employee		Società X	Approved	REOPEN
17		TO1SQ	Company Resource		Società X	Approved	REOPEN
18		F93066A	Company Employee		Società X	Approved	REOPEN
19		F99855D			Società X	Approved	LOCKED
20		NM319	Employee		Società X	Approved	REOPEN

Figura 3.10: Confronto con la lista post-rivalidazione

Queste tre utenze hanno avuto accesso a Z nonostante non fossero state indicate come approvate, l'applicativo è stato pertanto soggetto a alcuni casi di cattiva gestione dei diritti di accesso, tipologia di rischio descritto nel capitolo 2.6.1, per il periodo che è intercorso tra la fine del processo di rivalidazione (20.07.2022) e l'analisi effettuata da EY e dal management aziendale (02.11.2022).

Il referente dell'applicativo Z per la Società X è stato contattato prontamente per esporre il problema e, congiuntamente con la società sono stati valutati i rischi effettivi e potenziali e concordate le azioni mitigative.

Si riportano di seguito le specifiche casistiche relative alle diverse tipologie di situazioni.

1. Utenza F08611E

Tramite l'accesso del referente all'applicativo Z è stato possibile riscontrare che l'utenza F08611E era stata bloccata in data 21.07.2022 (vedi Figura 3.11). Non è stato inoltre effettuato dalla stessa alcun accesso a Z in data successiva al periodo di rivalidazione. Il pericolo è pertanto da dichiararsi rientrato, e il controllo concluso con esito positivo.

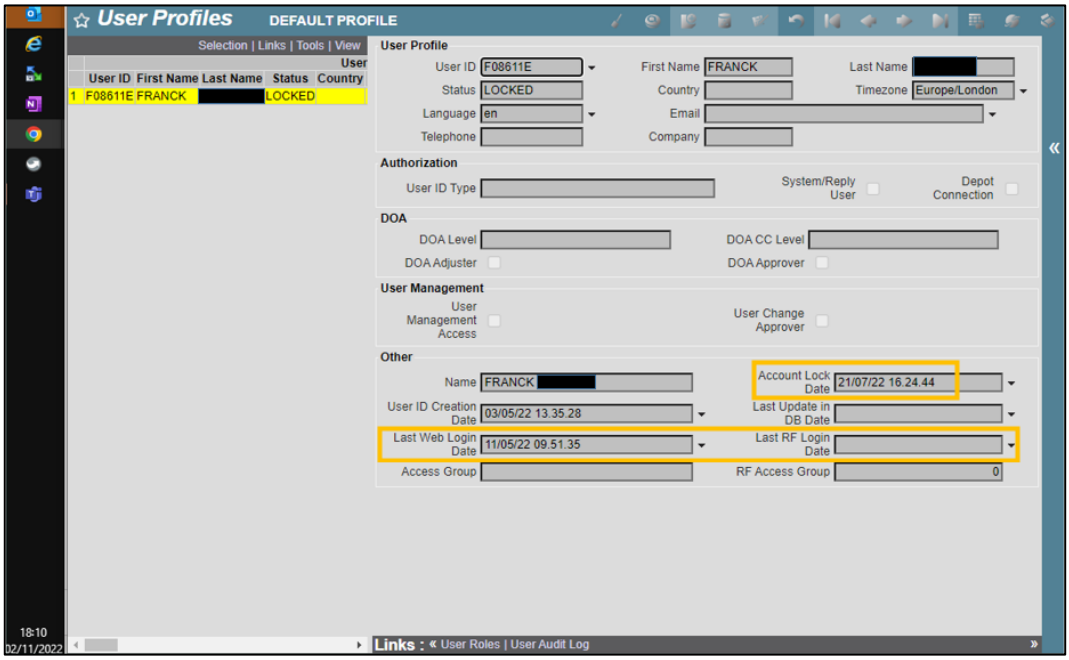


Figura 3.11: schermata dell'applicativo Z per l'utenza F08611E

Questa casistica rappresenta un rischio potenziale a cui è stato soggetto l'applicativo, ma per cui non è stata necessaria alcuna azione mitigativa.

2. Utenza F33057A

Accedendo all'applicativo Z per visualizzare lo stato dell'utenza F33057A (vedi Figura 3.12), è stato possibile notare che non era stata effettivamente revocata l'autorizzazione, in quanto risultava essere ancora in status 'REOPEN'. Attraverso i campi 'Last Web Login Date' e 'Last RF Login Date' è stato comunque riscontrato il fatto che l'utente non avesse effettuato alcun accesso all'applicativo durante il periodo in questione. Una richiesta di apertura ticket è stata intrapresa per segnalare la casistica e la necessaria chiusura dell'utenza in questione. Anche per lo user F33057A il controllo è stato quindi dichiarato concluso con esito positivo.

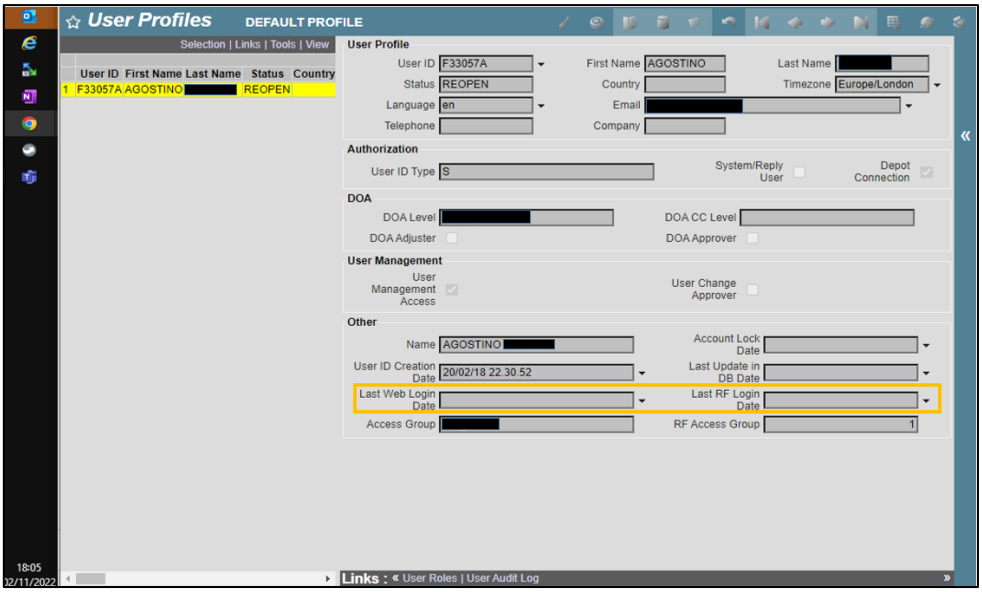


Figura 3.12: schermata dell'applicativo Z per l'utenza F33057A

Anche questa casistica rappresenta un rischio potenziale a cui è stato soggetto l'applicativo, tramite l'azione mitigativa concordata con la Società X è stato possibile evitare l'effettiva realizzazione del rischio.

3. Utenza F03016A

Dalla schermata di visualizzazione dell'applicativo Z per l'utenza F03016A (vedi Figura 3.13), è emerso che l'utenza, oltre ad essere ancora attiva, avesse effettuato un accesso in data successiva al processo di rivalidazione (25.10.2022 alle 05:32:19)

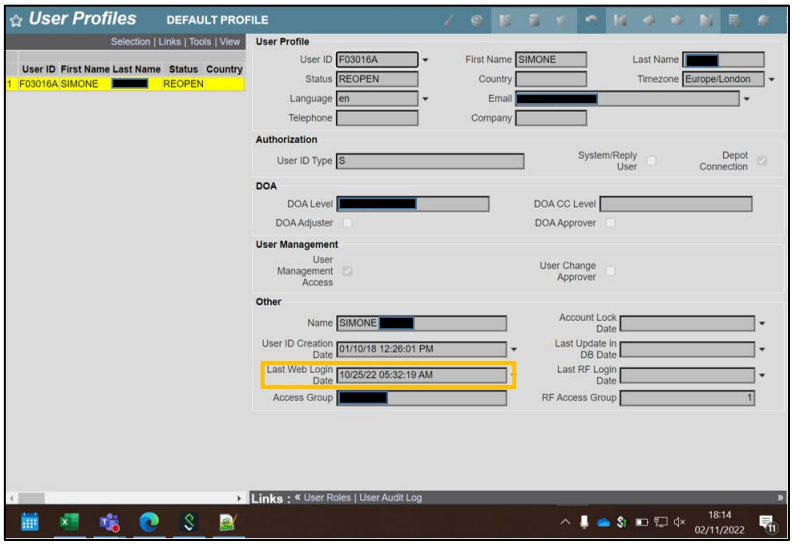


Figura 3.13: prima schermata dell'applicativo Z per l'utenza F03016A

È stato quindi portato avanti un ulteriore controllo. In Figura 3.14 è possibile vedere come l'utente F03016A, nonostante abbia effettuato un accesso all'applicativo, non ha eseguito alcuna modifica allo stock (attività principale regolata dall'applicativo Z).

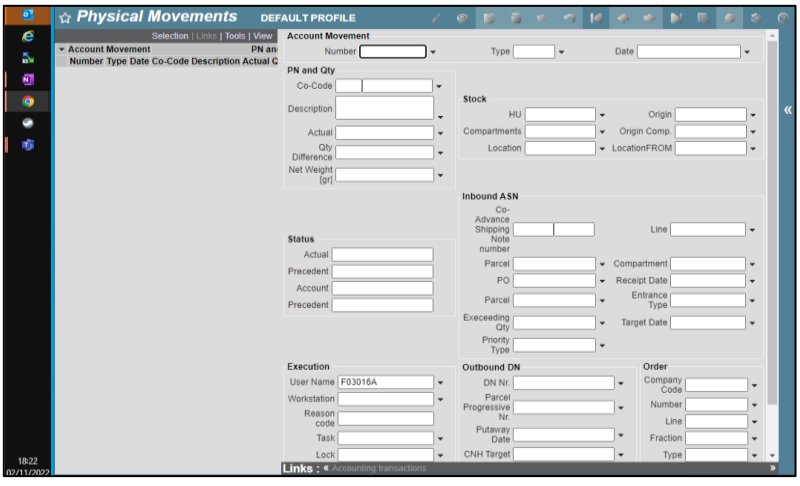


Figura 3.14: seconda schermata dell'applicativo Z per l'utenza F03016A

Il referente ha inoltre giustificato la casistica tramite una e-mail in cui dichiara di conferire lui stesso, in qualità di rivalidatore, l'accesso all'applicativo Z per l'utente F03016A. Durante il processo di rivalidazione il tool aveva indirizzato l'utenza a manager di Società esterne, motivo per cui non era stata correttamente rivalidata.

Questa circostanza ha determinato quindi l'identificazione di un issue risolta dalla società prima dell'anno di revisione di riferimento (2022).

Quest'ultima casistica è un rischio effettivo a cui la Società X è andata incontro. La mitigazione dello stesso, attraverso il supporto revisionale, rappresenta invece un caso tangibile in cui, un'organizzazione come EY, aiuta ad evitare situazioni che, potenzialmente, potrebbero danneggiare una società come X.

CAPITOLO IV

IL FUTURO: LA ROBOTIZZAZIONE DELL'AUDIT

4.1 INTRODUZIONE

Questo capitolo è incentrato sui possibili sviluppi futuri dei processi di audit, analizzando le innovazioni introducibili in questo mercato di servizi sempre alla ricerca della massima efficienza.

Contesti aziendali, caratterizzati da processi ridondanti ed applicativi che interagiscono in maniera non ottimale, sono sempre più comuni. Questa confusione organizzativa spesso limita lo sviluppo dell'azienda. L'aumento dei volumi dei dati e delle informazioni da gestire, deve essere affrontato attraverso una solida struttura organizzativa, altrimenti sono inevitabili l'aumento dei costi, i cicle time più lunghi del dovuto e la riduzione della qualità dell'output prodotto. Per convalidare che la soluzione a queste inefficienze potrebbe essere quella di integrare automazioni all'interno dei processi aziendali, saranno esaminati i vantaggi che l'introduzione della tecnologia avanzata è in grado di apportare, analizzando gli ambiti in cui ne è possibile l'applicazione.

La tecnologia e i processi di audit sono ad oggi sempre più connessi e dipendenti l'uno dall'altro. Controlli come il caso descritto nel capitolo III potrebbero essere resi completamente, o almeno parzialmente automatici, in modo da permettere alle risorse fisiche di concentrarsi esclusivamente su lavori in cui è richiesto maggior ragionamento. La robotica non deve essere vista come una soluzione di sostituzione dell'essere umano, bensì come uno strumento di supporto che semplifichi le operazioni routinarie caratterizzanti gran parte dei processi di audit.

4.2 LA ROBOTIC PROCESS AUTOMATION

La Robotic Process Automation (RPA), è definita come "un insieme di strumenti software in grado di automatizzare i processi aziendali basati sulle regole che coinvolgono attività routinarie, dati strutturati e risultati deterministici"[39]. Questi strumenti sono dei robot intelligenti, in grado di eseguire le attività che si ripetono all'interno dei processi, riuscendo così a interagire con gli applicativi sostituendo l'addetto fisico. In contesto di automazione robotica, con la parola robot, viene intesa una licenza software. Essi rappresentano delle entità silenziose, in grado di sostituire l'uomo in particolari situazioni.

La RPA rappresenta un'evoluzione dei sistemi di screen scraping, software progettati per poter prelevare in modo automatizzato contenuto e schermate di applicativi o siti. Questi sistemi sono già stati utilizzati in passato in contesti Audit con grandi quantità di dati, schermate e informazioni facilmente estraibili. Ad oggi, le piattaforme su cui si basa l'RPA, sono sufficientemente mature e affidabili per garantirne l'introduzione all'interno delle grandi società. Nello specifico un software RPA permette l'automatizzazione di attività semplici ma ricorrenti, precedentemente eseguite dall'auditor fisico attraverso delle interfacce utente. Esattamente come un essere umano, il robot, si interfaccia con un sistema IT, ma in modo molto più rapido e ad un costo decisamente inferiore. Le operazioni per cui sono sfruttati maggiormente gli automatismi sono il lancio di query, operazioni di trasporto dati, transcodifiche, button clicks o operazioni di merging. Questa tecnologia non invasiva può essere sovrapposta ai sistemi esistenti e integrata sfruttando i dati, riducendo al minimo le interruzioni della strategia e dell'architettura IT. La tecnologia RPA può iniziare con semplici attività basate su regole e scalare verso algoritmi più sofisticati e funzioni di apprendimento automatico man mano che l'organizzazione matura.[40]

---

[39] "Robotic Process Automation (RPA) emerges as software based solution to automate rules-based business processes that involve routine tasks, structured data and deterministic outcomes". S. Aguirre, A. Rodriguez, Automation of a Business Process Using Robotic Process Automation (RPA): A Case Study, Conference Paper, 2017.

[40] "Non-invasive technology can be laid over existing systems and integrated with existing data, minimizing disruption to existing IT strategy and architecture. RPA technology can begin with simple rules-based tasks, and scale to more sophisticated algorithms and machine-learning functions as the organization matures." RPA technology can begin with simple rules-based tasks and scale to more sophisticated functions as the organization matures, Detman Ordeman, EY, EMEIA Assurance Innovation and Digital Leader - EY

Basandosi sui ricavi ottenuti dalla vendita dei software RPA negli ultimi 6 anni[41] questo mercato risulta essere molto interessante e in forte crescita. Gli investimenti in costante aumento sui software RPA indicano come le organizzazioni stiano puntano a snellire il lavoro manuale e ripetitivo, in modo da permettere ai dipendenti di concentrarsi maggiormente su attività strategiche.

Year	Revenue ($ in millions)	Growth (%)
2016	250	-
2017	518,8	108%
2018	846,2	63%
2019	1411,1	67%
2020	1825	29%
2021	2389	31%
2022*	2854	19%

Tabella 4.1: Dati su ricavi e crescita rispetto all'anno precedente.

*Con * viene indicata una stima ad anno in corso*

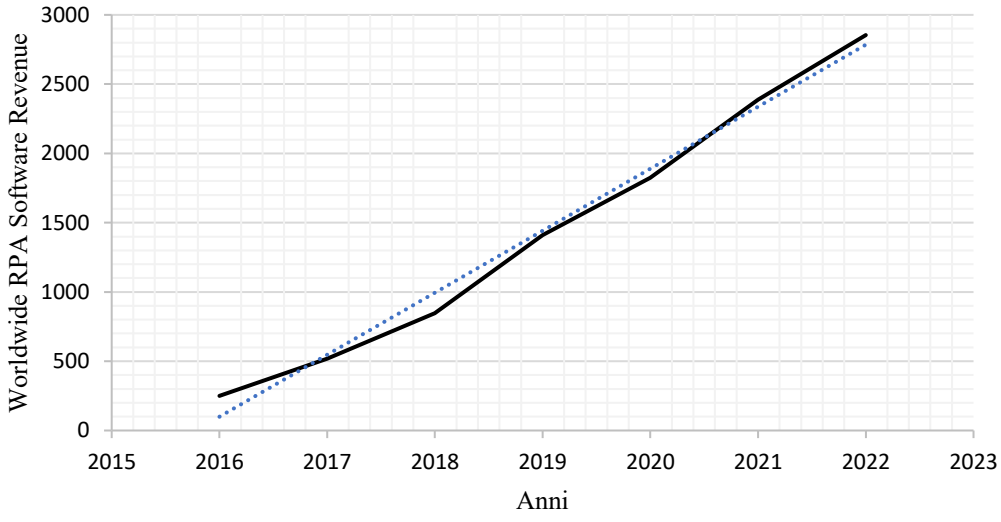


Grafico 4.1: Ricavi dalla vendita di Software RPA negli ultimi 6 anni

[41] Gartner Says Worldwide Robotic Process Automation Software Revenue to Reach Nearly $2 Billion in 2021, Stamford, Conn., September 2020; Gartner Says Worldwide Robotic Process Automation Software Market Grew 63% in 2018, Egham, U.K., June 24, 2019; The RPA Market Will Reach $2.9 Billion By 2021, Forrester, February 13th, 2017 e Gartner Says Worldwide RPA Software Spending to Reach $2.9 Billion in 2022, STAMFORD, Conn., August 1, 2022

Nel Grafico 4.2 è raffigurata la market size che questa tecnologia si prevede riuscirà a raggiungere entro il 2030.

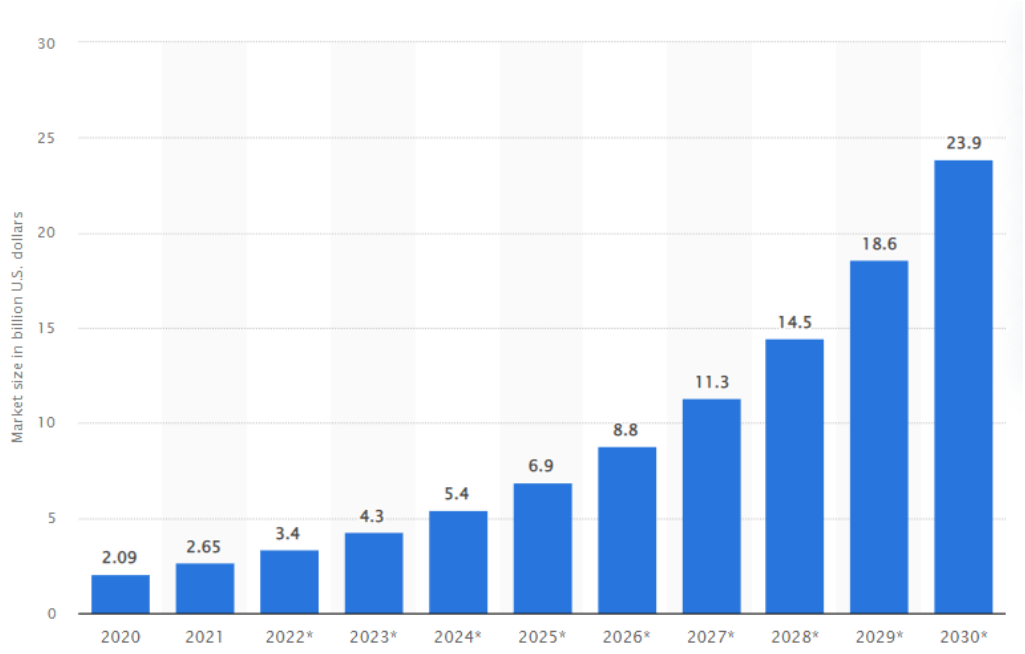


Grafico 4.2: Spending on robotic process automation (RPA) software worldwide from 2020 to 2030. Fonte: Statista

Per il mercato dell'automazione robotica dei processi (RPA), è prevista una crescita con un CAGR del 27,7% dal 2021 al 2030 fino a raggiungere un valore di 23,9 miliardi di dollari entro il 2030[42].

Le previsioni su questo mercato descrivono uno scenario in cui gli investimenti continueranno a crescere nel tempo. L'interesse di aziende della dimensione di Microsoft, che nel 2020 ha acquisito l'azienda Softomotive per rafforzare la legittimità del settore RPA, e UiPath, leader del settore che si dedica esclusivamente allo sviluppo di questi software, sono un'ulteriore prova delle potenzialità di questa tecnologia.

[42] "The robotic process automation (RPA) market was estimated to be worth 2.65 billion U.S. dollars in 2021. This market is forecast to grow with a CAGR of 27.7% from 2021 to 2030. The market size is expected to be valued at 23.9 billion U.S. dollars by 2030" Global RPA market size 2030 | Statista

La carta vincente della Robotic Process Automation è, senza dubbio, il risparmio dal punto di vista delle risorse, quindi del tempo e dei costi. Investire in una licenza RPA significa spendere l'equivalente anche solo di un quinto di stipendio di un dipendente medio[43] per riuscire a produrre, nello stesso tempo, l'equivalente del lavoro che può essere svolto da due a cinque persone[44]. Immaginando di acquistare una licenza, si potrebbero sostituire cinque persone, e quindi, spendendo un quinto, potrebbero essere sostituite venticinque persone con l'equivalente del costo di una sola risorsa. Questo calcolo è effettuato basandosi su ipotesi e, inoltre, non valuta il fatto che non tutte le attività possono essere svolte da un robot artificiale. Appare comunque interessante notare come la tecnologia sia molto più efficiente rispetto a un individuo in determinate circostanze e come essa continui a sostituire il lavoro umano con il passare del tempo.

I software RPA tengono inoltre traccia di tutte le attività svolte, limitando il numero di errori e consentendo di incrementare il livello di precisione di ogni task. Si riscontra pertanto un miglioramento non indifferente per quanto riguarda la qualità stessa del lavoro che verrebbe rivoluzionato. I software hanno il compito di svolgere le funzionalità di base di un'attività, in modo da eliminare la parte routinaria presente nella maggior parte degli audit, lasciando la fase in cui è necessaria una maggiore attenzione ai dettagli e un ragionamento più complesso ai dipendenti. Con questa struttura organizzativa, le attività che conferiscono maggior valore aggiunto ad una revisione verrebbero lasciate a figure professionali che avrebbero, inoltre, più tempo da poter investire. Conseguenza: un aumento sostanziale della produttività.

Riduzione dei costi, aumento della produttività, aumento della qualità e agevolazione rispetto al raggiungimento della conformità per le normative rappresentano i principali target che l'RPA permette di raggiungere.

---

[43] "Robotic automation can cost as little as 1/3rd of the price of an offshore full-time employee (FTE) and as little as 1/5th of the price of an onshore FTE". Capgemini Consulting, Robotic Process Automation-Robots conquer business processes in back offices, 2016.

[44] "One "robot" equals one software license and, in general, one robot can perform structured tasks equivalent to two to five humans". M. Lacity, L. Willcocks, What knowledge workers stand to gain from automation, Harvard Business Review,2015.

Si individuano inoltre i seguenti aspetti caratterizzanti questa tecnologia:

- Return on Investment (ROI): i tipici progetti RPA comprendono più progetti pilota funzionali, ma il programma viene completato in 9-12 mesi con un ROI inferiore a un anno.
- Right shoring: L'indipendenza geografica riduce la necessità di esternalizzare i lavori, pur garantendo un risparmio sui costi.
- Intersettorialità: Le procedure standardizzate rendono i processi compatibili tra i vari settori.[45]

[45] RPA technology can begin with simple rules-based tasks and scale to more sophisticated functions as the organization matures, Detman Ordeman, EY, EMEIA Assurance Innovation and Digital Leader - EY

4.2.1 RISPARMIO SUI COSTI

L'utilizzo dell'automatizzazione robotica permette una riduzione dei costi che può variare tra il 25% e il 50%. Un fattore da considerare è inoltre il fatto che i robot non vanno in vacanza: lavorando 24 ore su 24, 7 giorni su 7 senza giorni di ferie o festività garantiscono un rendimento, in proporzione, sempre superiore a quello delle risorse che lavorano 8 ore su 24 e 5 giorni su 7. I savings ottenibili dall'utilizzo dell'RPA permettono la diminuzione del lavoro intensivo svolto dagli esseri umani, che si tramuta in un risparmio di costo che a sua volta implica un guadagno tangibile per l'azienda.

Qualunque funzione IT ha come obiettivo l'ottimizzazione di tempi, risorse e qualità. Il trade-off tra queste tre caratteristiche rappresenta il problema che l'RPA permette di risolvere. Ipotizzando lo scenario di un progetto in ritardo, per cui è necessaria una conclusione a breve termine, l'unica soluzione possibile prevederebbe un aumento dei costi. È allo stesso tempo necessario riuscire a impattare il meno possibile su questi ultimi per questioni di budget. La diretta conseguenza sarà, quindi, una diminuzione delle risorse che però implica a sua volta un'inevitabile diminuzione della qualità. Ci troviamo di fronte a una situazione ricorrente in contesto aziendale in cui, per riuscire a diminuire le tempistiche progettuali viene sacrificata la qualità dell'output. Come dimostrato da casi reali relativi a situazioni in cui dovevano essere gestite situazioni di back office, volumi elevati e attività ripetitive di raccolta ed elaborazione dei dati[46], l'RPA si è dimostrata una soluzione. Nella pubblicazione "The IT Function and Robotic Process Automation"[47] vengono analizzate tre società Britanniche operanti nel settore dei servizi. Analizzando il caso particolare di una delle tre, appartenente al settore delle telecomunicazioni, appare evidente come l'RPA abbia permesso una soluzione descritta come 'Better, Faster For Less'. Dopo l'introduzione della RPA sono stati raggiunti livelli di automazione che hanno permesso una crescita del

[46] Mary Lacity, Leslie Willcocks and Andrew Craig (2015) on Robotic Process Automation at Telefonica O2 LSE Outsourcing Unit paper 15/03; Robotic Process Automation at Xchanging LSE Outsourcing Unit paper 15/03; and chapter on a major utility in Willcocks, L. and Lacity, M.(2016) Service Automation: Robots and the Future of Work (SB Publishing, Stratford).

[47] The IT Function and Robotic Process Automation, Paper 15/05, 2015, Professor Leslie Willcocks, Professor Mary Lacity and Andrew Craig. http://eprints.lse.ac.uk/64519/1/OUWRPS_15_05_published.pdf

business value dell'azienda, riducendo notevolmente i livelli di backlog dovuti alle scarse risorse impiegate per gestire enormi volumi.

4.2.2 AUMENTO DELLA QUALITA'

La tecnologia RPA garantisce un'accuratezza del 100% nelle attività automatizzate in cui viene utilizzata, offrendo servizi impeccabili ai processi che soffrono di alta probabilità di errore umano. L'affidabilità e la coerenza dei robot permettono di ridurre i casi di rielaborazione, spesso ricorrenti in contesti di audit, migliorando in questo modo esponenzialmente la qualità dell'output.

I robot vengono impostati su logiche ben precise, e regole inconfutabili che non permettono alcuna scelta da parte dell'automatismo. Se da un lato questo ne limita di molto il campo di applicazione, restringendolo a processi con tassi di eccezioni tendenti allo zero, dall'altro, rappresenta il motivo per cui la qualità dell'output è garantita. Per identificare eventuali violazioni o errori all'interno del sistema l'RPA esamina l'intera popolazione, cosa che invece il revisore normalmente fa attraverso lo studio di una porzione ridotta tramite un campionamento. Per avere un'idea sui test effettuati dai revisori fisici basta immaginare che, nella maggior parte dei controlli, vengono analizzati campioni pari al 20% della popolazione, senza mai superare i 25 records. Valutando l'intera popolazione tramite controlli a tappeto è invece garantito la correttezza del funzionamento del sistema di controllo interno.

Un'ulteriore differenza rispetto ai metodi tradizionali di revisione è riscontrabile nel trattamento dei dati, questi ultimi possono infatti essere analizzati contemporaneamente alla loro raccolta. La totalità della popolazione può quindi essere esaminata in modo continuo, riducendo a zero il rischio di campionamento. In questo modo nessun outlier può sfuggire ai controlli.

I software RPA hanno però dei limiti dettati dai campi di applicazione. Affinché possano essere applicati ad un processo aziendale quest'ultimo deve soddisfare determinate caratteristiche:

- avere elevati volumi di elaborazione dati, caratteristica propria di attività frequenti e ricorsive;
- i compiti ad esso connessi non devono necessitare né di un giudizio né di un'interpretazione soggettiva, devono presentare bassi livelli cognitivi;
- presentare raramente delle eccezioni, se non quelle dovute a errori umani;
- essere connesso a più applicativi, in modo da permettere una maggiore velocità nel reperire le informazioni;

Queste caratteristiche, che definiscono dei processi aziendali ben precisi, rappresentano il limite di cui ad oggi soffre l'RPA. Per superarli è in corso una continua evoluzione architetturale, attraverso metodi come il 'Machine Learning', che permette un miglioramento della tecnologia costante e, come indica il nome stesso, automatico. A questo punto, una domanda sorge spontanea: com'è possibile che un sistema robotizzato si migliori da solo? Per dare una risposta a questa domanda è necessario studiare la struttura che sta dietro questa particolare tecnologia e le modalità con cui gli algoritmi riescono a imparare sfruttando i dati che gli vengono forniti.

4.3 EVOLUZIONE DELL'AUTOMAZIONE

Il concetto di Machine Learning (ML) nasce nel 1959 da un'intuizione di Arthur Samuel che lo definì come "a field of study that gives computers the ability to learn without being explicitly programmed".

L'ML rappresenta un sottoinsieme dell'intelligenza artificale (IA), che ha il preciso compito di configurare sistemi in grado di apprendere e migliorare le performance utilizzando i dati stessi che elaborano nello svolgere le attività per cui sono programmati (Figura 4.1). Viene identificato come intelligenza artificiale, invece, un qualsiasi sistema informatico che limiti il modo in cui vengono prese delle decisioni da un essere umano.

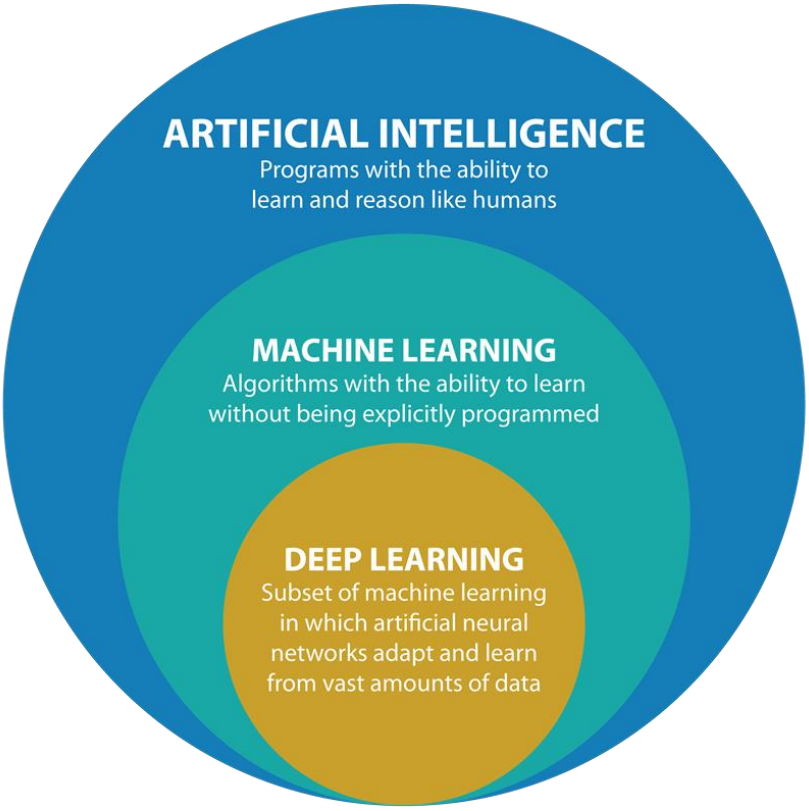


Figura 4.1: Sottoinsiemi dell'Intelligenza arificiale. Fonte: https://www.zekiah.com/insights/data-analytics/an-introduction-to-deep-learning-machine-learning-and-ai

Un ulteriore sottoinsieme, sia di Intelligenza Artificiale che di Machine Learning è rappresentato dal cosiddetto Deep Learning (DL), o apprendimento profondo. Esso rappresenta il cervello di un algoritmo e viene infatti definito come "una tecnica di apprendimento in cui si espongono reti neurali artificiali a vaste quantità di dati, in modo che possano imparare a svolgere compiti"[48]. Il DL è composto da più livelli in cui sono presenti modelli di apprendimento che hanno il compito di trasformare i dati in input (basso livello) in informazioni più 'astratte' (alto livello). In questo modo i dati vengono organizzati seguendo un ordine gerarchico basato sul livello di astrazione.[49]

L'ML è applicabile a problemi e set di dati diversi. Un esempio dell'efficacia di questo metodo è rappresentato dagli algoritmi presenti nella maggior parte di applicativi che gestiscono il flusso delle e-mail, in particolare, dalla parte di software che riconosce e limita la ricezione di spam o contenuti riconducibili a frodi. Questi applicativi sfruttano i principi del Machine Learning, e intervengono autonomamente senza necessitare di un intervento umano.

Il Machine Learning può essere applicato a un algoritmo seguendo 3 diverse tecniche:

- Apprendimento supervisionato: l'algoritmo sfrutta i dati associati a risposte e informazioni esistenti. Immagazzinano questi dati si 'prepara' a situazioni future simili, in cui è possibile associare come output le stesse risposte. Una forma di apprendimento simile a quello dei bambini che associano, vedendo ripetutamente azioni simili dei propri genitori, una regola generale. Questa struttura è la più diffusa.
- Apprendimento non supervisionato: in questo caso l'algoritmo si migliora partendo esclusivamente da esempi privi di risposta associata. Esso stabilisce autonomamente i pattern dei dati, ovvero un campione di dati che veicola un'informazione unica. Attraverso questa configurazione viene permesso all'algoritmo di rielaborare i dati in modo diverso per effettuare

[48] Redazione Osservatori Digital Innovation, Alla scoperta del Deep Learning: significato, esempi e applicazioni, 2019, Osservatori.net
[49] Y. LeCun, Y. Bengio, G. Hinton, Deep Learning, Nature, 2015.

analisi future. Questa tecnica è meno diffusa rispetto all'apprendimento supervisionato, in quanto è molto più complessa dovendo fornire delle informazioni ignote.

- Apprendimento per rinforzo: anche in questo caso i dati raccolti dall'algoritmo sono privi di risposte associate, e le risposte sono frutto delle scelte dell'algoritmo scelto come nell'apprendimento senza supervisione. La differenza sta nel fatto che l'algoritmo riceve dei feedback, sia positivi che negativi, attraverso l'interazione con altri ambienti esterni. Questa struttura è sfruttata particolarmente in programmi in cui sono richiesti dei calcoli automatici e ricorsivi come nei giochi.

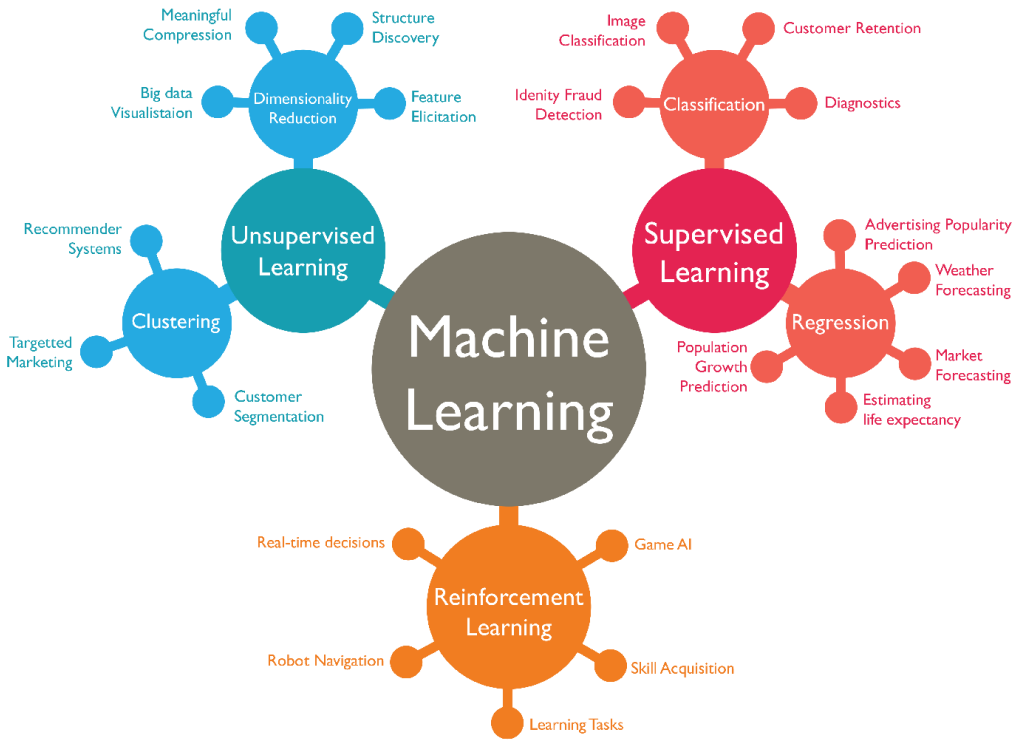


Figura 4.2: Tecniche di Machine Learning. Fonte : [10 Companies Using Machine Learning in Cool Ways (wordstream.com)]

Intelligenza artificiale e RPA rappresentano entrambe soluzioni per l'automazione in contesti di audit pur avendo due funzionamenti differenti.

La differenza principale sta nella tipologia di processi su cui sono applicabili le due tecnologie. Mentre un software RPA è applicabile solo a processi routinari e basati su regole standardizzate, l'AI può essere utilizzata per risolvere situazioni anche non di routine e richiedenti ragionamento. Il machine learning, inoltre, garantisce all'intelligenza artificiale un continuo apprendimento nel tempo cosa che non è propria dei software RPA.

Il limite dell'intelligenza artificiale è però la difficoltà che sta dietro la costruzione di questi algoritmi molto difficili da automatizzare e quindi richiedono molto tempo. Concentrandosi su funzioni più complesse rispetto agli automatismi gestiti dall'RPA, permette indiscutibilmente di creare valore ma la sua implementazione richiede un investimento di gran lunga superiore.

Unendo le due tecnologie è possibile ottenere l'Intelligent Automation. I robot sarebbero in grado di sostituire un individuo anche in processi per cui è richiesto del ragionamento, riuscendo, contemporaneamente, a risolvere i task ripetitivi velocemente e autonomamente, riducendone drasticamente i tempi e i costi.

AI e RPA apporteranno enormi cambiamenti all'interno dei processi di revisione legale. L'informatizzazione delle attività di revisione rivoluzionerebbe il mondo dell'auditing, limitando ancora di più il rapporto con il cliente, rendendo quindi quasi indifferente una società di revisione rispetto a un'altra. Il criterio decisionale sarebbe esclusivamente il prezzo della consulenza.

Inoltre, il ruolo degli auditor diventerebbe esclusivamente quello di controllare il lavoro eseguito dagli automatismi, senza alcun rapporto diretto con il cliente, che non sarebbe più in grado di fornire un feedback sull'azienda, ma sulla sua tecnologia.

Se da un lato è vero che l'introduzione della tecnologia rende il processo molto più veloce ed efficiente, dall'altro, la diminuzione del tempo necessario per il

completamento degli stessi tasks potrebbe significare una minor remunerazione per i revisori.

Questa prospettiva potrebbe portare ad un maggiore tasso di disoccupazione degli auditor, che significherebbe meno costi per la società, ma anche un ulteriore rischio. I clienti in grado di cogliere questa informazione inizierebbero ad avere una willingness to pay decisamente inferiore, [50] dando inizio ad un'inevitabile diminuzione dei profitti ottenibili.

In ottica di lungo periodo, un settore di revisione legale più informatizzato potrebbe dare più spazio all'ambito della consulenza che risulta essere anche più redditizio. Questo potrebbe permettere di coprire la diminuzione delle entrate nei campi di audit.

Anche l'aspetto di disoccupazione potrebbe essere meno grave del previsto poiché le tecnologie di intelligenza artificiale sostituiscono compiti specifici piuttosto che interi posti di lavoro, la perdita di occupazione nel breve termine sarà probabilmente relativamente lenta e marginale piuttosto che drammatica.[51]

Sarebbe sicuramente inevitabile anche una rivoluzione nei ruoli dei revisori, in quanto figure specializzate in ambiti specifici sarebbero sempre più ricercate. Diminuirebbe di gran lunga la richiesta di figure junior, che invece oggi rappresentano un punto chiave della strategia di questa tipologia di aziende.

La velocità di espansione delle automazioni in questo ambito rappresenterà una grande sfida anche per gli enti che regolamentano le revisioni, che saranno chiamati ad aggiornare gli standard in modo da essere adatti ad un contesto più virtuale. Se le società di revisione come le "Big-Four" non avranno difficoltà ad affrontare l'innovazione, dato l'ingente capitale sia umano che finanziario, le dirette

[50] "If auditors can capture a large proportion of the value generated by automation, their profits could increase. However, if clients become aware of the extent of these cost savings, their willingness to pay high auditing fees might decrease. If auditors are forced to wholly or largely pass cost reductions to clients in the form of lower fees, amortizing IT investments would become more difficult, and profits would remain stable or even sink." V. Tiberius, S. Hirth, Impacts of digitization on auditing: A Delphi study for Germany, Journal of International Accounting, Auditing and Taxation, 2019.

[51] "Since AI technologies replace specific tasks rather than entire jobs, loss of employment in the short term is likely to be relatively slow and to be marginal rather than dramatic". J. Kokina, T. H. Davenport, The Emergence of Artificial Intelligence: How Automation is Changing Auditing, Journal of Emerging Technologies in Accounting, 2017.

concorrenti, invece, non avranno risorse sufficienti per riuscire a stare al passo.[52] A causa delle ingenti risorse che queste società dispongono, si andrà incontro ad un innalzamento delle barriere all'entrata per gli elevati costi della tecnologia che, viceversa per le quattro, non rappresenterebbe alcun problema. Il mercato vedrebbe quindi l'uscita dei player più piccoli, marcando, col tempo, sempre di più la differenza tra le poche società giganti del settore e le altre.

[52] H. Agnew, Auditing: Pitch battle, Financial Times, 2016.

CONCLUSIONI

Il presente lavoro di tesi, dopo aver identificato i radicali cambiamenti avvenuti in ambito Audit IT, è stato strutturato attraverso un'analisi interna e diretta su progetti di revisione contabile, intrapresi dall'azienda con cui ho collaborato negli ultimi mesi.

Preso atto degli avvenimenti storici che hanno segnato il contesto revisionale, l'obiettivo è stato quello di studiare i meccanismi che hanno portato all'odierna organizzazione aziendale. La crescita della domanda per questa tipologia di servizi ha portato a un'evoluzione dell'intero settore, che ad oggi, continua a investire in soluzioni tecnologiche sempre più all'avanguardia.

L'ipotesi argomentativa, che ha ispirato il lavoro della tesi proposta, è stata sviluppata in quattro capitoli, ciascuno dei quali ha consentito di giungere a conclusioni in progress, fondamentali per l'avanzamento dello studio trattato nel capitolo consecutivo.

Precisato lo scopo di un audit, in modo da comprendere perché abbia assunto una funzione sempre più importante all'interno di un'azienda, sono stati analizzati gli scenari che hanno guidato il cambiamento, a partire dalla visione generale del mercato americano prima dell'introduzione della normativa SOX.

Analizzando i processi e i rischi che devono essere affrontati, individuando gli strumenti a supporto delle società che implementano i controlli e analizzando i punti di forza delle principali società operanti a livello globale, è stato possibile fornire un'idea d'insieme dell'ambiente preso in considerazione.

Sono state quindi fornite evidenze a dimostrazione del fatto che, il lavoro di audit, permette alle aziende di ottenere un valore aggiunto tangibile, in termini di sicurezza legata al rischio tecnologico.

A conclusione del lavoro di tesi, condotto in approfondimento della contemporanea esperienza lavorativa, sono state tracciate le modalità esplicative che rappresentano i punti di forza delle aziende operanti in questo settore. Attraverso i processi di

controllo è possibile fornire un supporto fondamentale a clienti terzi, e convalidare così un importante miglioramento in termini di organizzazione aziendale ed efficienza. L'intento proposto a conclusione dell'ipotesi di studio elaborata nel presente lavoro di tesi, è quello di lasciare al lettore informazioni sugli orientamenti verso cui, con ogni probabilità, si muoverà questo particolare settore del mercato di servizi.

BIBLIOGRAFIA

Agnew, H. (2016). Auditing: Pitch battle. Financial Times. https://www.ft.com/content/268637f6-15c8-11e6-9d98-00386a18e39d

Aguirre, S., Rodriguez, A. (2017). Automation of a Business Process Using Robotic Process Automation (RPA): A Case Study, Conference Paper. Published in Workshop on Engineering Application. Computer Science, Business. Springer International Publishing AG 2017J.C. Figueroa-García et al. (Eds.): WEA 2017, CCIS 742, pp. 1–7, 2017.DOI: 10.1007/978-3-319-66963-2_7.

Associazione Italiana Information Systems Auditors AIEA Capitolo di Milano di ISACA. (2006). Obiettivi di controllo IT per il Sarbanes_Oxley Act, 2° Edizione, il ruolo dell'IT nel progetto e nell'implementazione dei controlli interni per la predisposizione del reporting finanziario.

Associazione politico culturale Marx21. (2006). Caso Enron, ovvero l'epilogo giudiziario della fama creativa. https://www.marx21.it/archivio/articoli-archivio/caso-enron-ovvero-lepilogo-giudiziario-della-finanza-creativa/.

Balzarotti, L., Miccolupi, B. (2016). La truffa di Enron, 15 anni fa. Le tappe del default nelle pagine d'Archivio. https://www.corriere.it/extra-per-voi/2016/12/02/truffa-enron-15-anni-fa-tappe-default-pagine-d-archivio-7b487b7a-b7f6-11e6-a82f-f4dafb547583.shtml.

Capgemini Consulting. (2016). Robotic Process Automation-Robots conquer business processes in back offices. A 2016 study conducted by Capgemini Consulting and Capgemini Business Services. https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/robotic-process-automation-study.pdf. DOI: 10.2308/jeta-51730.

Fung, H., P. (2014). Criteria, use cases and effects of information technology process automation (ITPA). Advances in Robotics & Automation. Vol. 3. School of Management, Asia e University, Kuala Lumpur, Malaysia.

Goasduff, L. (2022). Gartner Says Worldwide RPA Software Spending to Reach $2.9 Billion in 2022. STAMFORD, Conn., August 1, 2022 https://www.gartner.com/en/newsroom/press-releases/2022-08-1-rpa-forecast-2022-2q22-press-release.

Johnson, Z. (2019). An introduction to Deep Learning, Machine Learning and AI. https://www.zekiah.com/insights/data-analytics/an-introduction-to-deep-learning-machine-learning-and-ai. ZechiaTech.

Kokina, J., Davenport, T. H. (2017). The Emergence of Artificial Intelligence: How Automation is Changing Auditing. Journal of Emerging Technologies in Accounting. April 2017Journal of Emerging Technologies in Accounting 14(1)
LeCun, Y., Bengio, Y., Hinton, G. (2015). Deep Learning, Nature. Nature Volume 521, 436–444.

Massaron, L., Mueller, J., P. (2020). Intelligenza Artificiale for dummies. Ulrico Hoepli Editore S.p.A., Milano.

Moore, S. (2019). Gartner Says Worldwide Robotic Process Automation Software Market Grew 63% in 2018. EGHAM, U.K., June 24, 2019 https://www.gartner.com/en/newsroom/press-releases/2019-06-24-gartner-says-worldwide-robotic-process-automation-sof.

Najafabadi, M.M., Villanustre, F., Khoshgoftaar, T.M. et al. (2015). Deep learning applications and challenges in big data analytics. Journal of Big Data 2, 1. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-014-0007-7.

Ordemann, D. (2017). Why robotics-led finance could signal the dawn of a new partnership. Ernst & Young. EY EMEIA Assurance Innovation and Digital Leader https://www.ey.com/en_gl/assurance/why-robotics-led-finance-could-signal-the-dawn-of-a-new-partners.

PCAOB Release No. 2005-023. (2005). https://pcaobus.org/Inspections/Documents/2005_11-30_Release_2005-023.pdf#:~:text=Auditing%20Standard%20No.%202%20requires%20the%20auditor%20to,effective%20and%20efficient%20way%20to%20accomplish%20these%20objectives.

Rimol, M., Costello, K. (2020). Gartner Says Worldwide Robotic Process Automation Software Revenue to Reach Nearly $2 Billion in 2021. STAMFORD, Conn., September 21, 2020. https://www.gartner.com/en/newsroom/press-releases/2020-09-21-gartner-says-worldwide-robotic-process-automation-software-revenue-to-reach-nearly-2-billion-in-2021.

Sarbanes-Oxley Act. (2002). https://sarbanes-oxley-act.com.

Sibalija, T., Jovanovic, S. (2019). Robotic Process Automation: Overview and Opportunities. International Journal "Advanced Quality", Vol. 46, N. 3-4, 2018. year, Belgrade, Serbia.

Tiberius, V., Hirth, S. (2019). Impacts of digitization on auditing: A Delphi study for Germany, Journal of International Accounting, Auditing and Taxation. November 2019 Journal of International Accounting Auditing and Taxation 37:100288. DOI: 10.1016/j.intaccaudtax.2019.100288.

Torlone, T., Howell, R., Ip, F., Mahajan, A. (2016). Robotic Process Automation: The Power of Automation. PwC. https://www.pwc.lu/en/rpa/docs/robotics-process-automation.pdf.

Willcocks, L., Lacity, M., Craig, A. (2015). The IT Function and Robotic Process Automation. The Outsourcing Unit Working Research Paper Series (15/05). The London School of Economics and Political Science, London, UK.