POLITECNICO DI TORINO

Dipartimento di Ingegneria Gestionale e della Produzione

Corso di Laurea Magistrale in Ingegneria Gestionale

Tesi di Laurea Magistrale

La figura dell'IT Auditor: critiche e scenari futuri

Relatore:

Prof. Emilio Paolucci

Candidata:

Gemma Gualtieri

Anno Accademico 2019-2020

Sommario

ABSTRACT

Il seguente lavoro di tesi partirà illustrando la figura del revisore legale dei conti, nel quadro del sistema capitalistico, il quale assume una posizione di garante della trasparenza e della veridicità dei bilanci contabili. L'attenzione sarà posta sui sistemi informativi che, data la crescente complessità dei processi aziendali, sono indispensabili per supportare la rendicontazione finanziaria e contabile e per garantire maggiore correttezza. Con il tempo, infatti, il sistema contabile si è trasformato da solo raccoglitore ed elaboratore di dati di natura contabile ed economica a polmone informativo principale di tutta l'azienda. Da qui l'importanza di monitorare i rischi che intaccano i sistemi informativi, quindi la necessità di una figura ad hoc quale IT Auditor che fornisce valutazioni di adeguatezza e sicurezza dei sistemi informativi a supporto dei processi fiscali e contabili ed indica mirati piani di miglioramento per aumentare l'efficacia e la robustezza dei sistemi IT.

Sono descritte nel secondo capitolo le procedure attuate per revisionare i controlli interni effettuati dalle società al fine di garantire l'integrità delle informazioni finanziarie e contabili, promuovere la responsabilità e prevenire le frodi.

Data la ripetitività delle attività effettuate dall'IT auditor si è valutato l'impatto che potrebbe avere l'automatizzazione di parte di esse tramite RPA (Robotic Process Automation). Una volta introdotto il processo di automazione, sarà effettuata un'analisi volta ad evidenziare benefici e rischi emergenti dal nuovo scenario tecnologico.

Il focus dell'analisi verterà sul cambiamento tecnologico e sul suo impatto in termini di costi, tempi, qualità e struttura organizzativa. L'obiettivo è quello di dimostrare che l'automazione non si traduce in una semplice sostituzione di capitale umano, quanto piuttosto in una vera e propria opportunità di eliminare mansioni meccaniche e ripetitive per le risorse umane consentendo ad esse di concentrarsi a svolgere attività più significative e strategiche su cui il "tocco" umano risulta ancora indispensabile.

INTRODUZIONE

L'attendibilità dei bilanci è fondamentale nel quadro del sistema capitalistico poiché garantisce che i rapporti tra coloro che governano le aziende e le diverse categorie di terzi interessati alle sorti aziendali si svolgano nel rispetto dei reciproci diritti e doveri. La parola chiave per il successo è la trasparenza delle informazioni e dei dati trasmessi.
Una maggiore trasparenza implica fiducia degli stakeholders che si traduce in una crescita sostenibile e in una posizione solida nel settore.

Per ottenere la trasparenza i processi di rendicontazione finanziari sono stati informatizzati il più possibile per ridurre l'errore umano nelle registrazioni contabili.
La rendicontazione finanziaria, ovvero tutti i processi di registrazione, sintetizzazione e accumulo delle transazioni è effettuata infatti da elaboratori con applicazioni e software dedicati.
Tuttavia, non è sufficiente affidarsi alla sola tecnologia in quanto le applicazioni e i sistemi hanno controlli programmati al loro interno che, se sono critici, devono essere

monitorati e valutati attentamente, in particolare quando il management fa affidamento su di essi con una verifica dell'utente limitata o assente dei risultati dell'elaborazione.
Nell'ambiente IT, infatti, esiste una serie di rischi legata all'accesso da parte di individui a software, hardware e componenti dell'ambiente tecnologico inerenti all'uso di modifiche non autorizzate o imperfette ai programmi che possono introdurre errori o causare elaborazioni incomplete.
Tale serie di rischi deve essere gestita per il monitoraggio e la salvaguardia dei processi aziendali e per la valutazione del controllo interno.

È qui che si inserisce la revisione legale dei conti che riveste nei tempi moderni, un'importanza fondamentale e strategica oltre che determinante, in un percorso guidato di crescita e sviluppo economico-imprenditoriale o commerciale, teso ad acquistare, mantenere e potenziare una posizione solida nel mercato, oltre che mitigare il rischio finanziario (variazione della liquidità aziendale) sempre presente in esso.

Il revisore legale dei conti nell'espletamento dell'incarico ad esso conferito, assume infatti un ruolo preminente, determinante e insostituibile, che nel corso degli ultimi anni si è consolidato maggiormente attraverso un passaggio cruciale imprescindibile: da mero "arbitro" dell'attendibilità sostanziale del bilancio a "garante" indiscusso della qualità dell'informativa contabile che tende a proteggere e tutelare in maniera pressante ciò che può essere senz'altro definito un "Bene Pubblico", coinvolgendo una pluralità numerosa di soggetti.[1]

Si instaura, quindi, attraverso la procedura di revisione, un duplice rapporto di agenzia, dove il primo legame si realizza tra management e azionisti, mentre il secondo tra azionisti e soggetti che svolgono la revisione, riproponendo problemi di monitoraggio e incentivazione in merito alle informazioni contabili, potendo queste ultime essere manipolate e modificate per scopi ulteriori e diversi rispetto il controllo stesso.

[1] Roberto Ercoli, 19 Aprile 2019, *Il controllo di qualita' nella revisione: normativa e novità*, la REVISIONE LEGALE, https://www.larevisionelegale.it/2019/04/19/il-controllo-di-qualita-nella-revisione-normativa-e-novita/

Negli ultimi anni, infatti, non è possibile non considerare un cambiamento strutturale anche implicito nella stessa riformulazione dei Principi di Revisione, che si vanno evolvendo nel corso del tempo, rimodellandosi da semplici a complessi. Si sta passando infatti da un'attività di controllo basata sui meri, puri e semplici saldi di bilancio, a un'attività di revisione che valuta in maniera più generale, ampia, estesa, ma nel contempo, minuziosa e attenta, l'attività aziendale nel suo complesso con particolare attenzione ai Rischi d'impresa che incidono e si trasferiscono al bilancio d'esercizio, innescando un coinvolgimento pieno e concreto di tutte le funzioni, aree e attività aziendali nel procedimento di controllo. Su questa strada procederà la revisione legale, orientata alla massima collaborazione e trasparenza delle informazioni, scavalcando i tradizionali vincoli e barriere tra reparti e funzioni aziendali diversi tra loro, in un'ottica di miglioramento continuo.

Il revisore legale dei conti per fare ciò dovrà perseguire obiettivi fondamentali quali[2]:

- *Funzione Preventiva*, ovvero essere capace di cogliere in tempo sintomi degenerativi di una situazione aziendale da cui potrebbero scaturire potenziali e gravi ripercussioni negative sia rispetto l'ambiente interno all'azienda e al contenuto e all'immagine aziendale (aspetto reputazionale), sia riguardo quello esterno all'azienda e che fa diretto riferimento agli attori terzi ma funzionali alla stessa presenza dell'impresa sul mercato
- *Funzione di Controllo*, che fa riferimento alla possibilità, qualora ve ne fossero, di accertare e verificare azioni fraudolente, o indagare su fondati sospetti di comportamenti scorretti e quindi fornire dettagliate informazioni al "Pubblico" sulle risultanze stesse del controllo (funzione pubblicistica) ma anche funzione di controllo per l'ottenimento dell'ammissione alla quotazione delle azioni ai mercati regolamentati.
- *Funzione di Supporto* alle valutazioni dell'azienda o rami di essa circa operazioni straordinarie d'impresa fra cui Cessioni, Scorporazioni, Fusioni, Scissioni o sulla compravendita di rilevanti pacchetti azionari secondo logiche imprenditoriali-commerciali qualora non addirittura speculative.

[2] Mirko Alchirafi, 2011, Tesi di Laurea in Economia e commercio, *Indipendenza e conflitto d'interessi nella revisione legale dei conti: qualità ed evoluzione delle funzioni del revisore alla luce delle recenti riforme*

- *Funzioni di Verifica* sull'operato degli amministratori e sulla correttezza di questi ai fini di una massima tutela e protezione dei creditori sociali e dei soci di minoranza.
- *Funzione di Garanzia* sull'attendibilità del principale documento contabile, il Bilancio d'esercizio, in particolare rispetto all'amministrazione fiscale centrale e i soggetti finanziatori (specie banche e istituti di credito).
- *Funzione di Tutela* degli Interessi superiori degli azionisti, sia patrimoniali che economici.
- *Funzione di Valutazione* oggettiva dei rischi intrinseci aziendali attraverso controlli mirati sia quantitativi che qualitativi sui dati aziendali. L'efficacia dei controlli intorno alle applicazioni e ai sistemi influisce, infatti, direttamente sull'integrità del trattamento dei dati e sulle informazioni che sono riportate al completamento dell'elaborazione.

Attraverso il perseguimento di tali funzioni l'attività del revisore legale infonde vantaggi e benefici effettivi sulle diverse aree gestionali, contribuendo a eliminarne ed eroderne i difetti e migliorando il funzionamento e la "produttività".

CAPITOLO 1

1.1 L'importanza della trasparenza del bilancio e il ruolo dei sistemi informativi

Il bilancio d'esercizio ha lo scopo di offrire informazioni esaustive e complete sulla gestione aziendale agli utilizzatori e a tutti coloro che in qualche modo sono interessati ad esso.
Nella redazione del bilancio devono essere rispettati dei principi fondamentali, quali:

- La chiarezza, ovvero il bilancio deve essere comprensibile a tutti gli stakeholders e trasparente
- La veridicità, nel senso che le quantità oggettive devono essere vere e le stime devono essere attendibili
- La correttezza, che si riferisce all'applicazione corretta dei principi contabili ovvero delle norme e delle regole amministrative

L'articolo 243 *bis* del Codice Civile tratta specificamente dei Principi di redazione del bilancio sottolineando nel comma 1 che la valutazione delle voci deve essere fatta secondo prudenza e nella prospettiva di continuazione dell'attività aziendale.
Scopo della prudenza è di evitare di sovrastimare le voci, ragione per cui si traduce in due sottoprincipi:
- Gli utili "sperati" non devono essere inseriti nel bilancio
- Le perdite "presunte" devono essere inserite nel bilancio.

Nel comma 1-bis si sottolinea la trasparenza in quanto si richiede che la rilevazione delle voci sia effettuata tenendo conto della sostanza dell'operazione o del contratto.[3]

Il bilancio esplica le condizioni di liquidità rispetto ad una precisa situazione patrimoniale ed in modo approssimato le entrate e le uscite che si presenteranno nel breve futuro, ovvero subito dopo la chiusura del fiscal year.

[3] Art. 243-bis, Principi di redazione del bilancio, Codice Civile

Da qui si rileva il primo limite informativo del bilancio verso gli stakeholders, ovvero di evidenziare la situazione finanziaria nel breve periodo. Il bilancio non è in grado infatti di individuare le future entrate ed uscite e le necessità di finanziamento che l'impresa richiederà nel futuro.

Il secondo limite è quello di presentare la situazione economica confinata nel lasso temporale di anno. Ma ciò che conta per la sopravvivenza dell'impresa è che l'equilibrio tra costi e ricavi sia mantenuto nel medio e lungo periodo.

Il terzo limite è quello di presentare la situazione patrimoniale nell'ipotesi di continuità, ovvero di funzionamento. Tuttavia, lo scopo dovrebbe essere quello di capire la composizione del capitale e le sue variazioni nel tempo, per indagare su come potrebbe essere utilizzato per la creazione di nuovo valore.

Visti questi limiti, il bilancio deve riuscire a offrire le medesime informazioni minime a tutti gli interessati, pur non riuscendo ad offrire una visione completa di tutte le sue voci.
Il bilancio deve consentire di:

- Appurare e valutare la consistenza del patrimonio di funzionamento e le variazioni avvenute durante il fiscal year preso in considerazione.
- Esprimere come le funzioni e i settori costituenti l'impresa impattano sul risultato economico ottenuto.
- Mostrare una visione globale della situazione finanziaria dell'impresa inerente al fiscal year preso in esame.

Per supportare la rendicontazione finanziaria e contabile e per garantire una maggiore correttezza, a partire dagli anni sessanta con l'aumentare della complessità dei processi aziendali, si è iniziato ad utilizzare i sistemi informativi.
Con il tempo il sistema contabile si è trasformato da solo raccoglitore ed elaboratore di dati di natura contabile ed economica a polmone informativo principale di tutta l'azienda.[4]

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

Il sistema informativo contabile è costituito non solo da un insieme di dati elementari e da aggregazioni e scomposizione di essi, ma anche da elaborazioni contabili e statistiche utili all'azienda per determinare il patrimonio di funzionamento, il risultato d'esercizio e per le dichiarazioni ai fini fiscali. In secondo luogo è funzionale come supporto alle decisioni imprenditoriali e per il monitoraggio delle attività.
Un sistema informativo contabile, permette quindi non soltanto di trattare la contabilità generale ma anche le contabilità speciali quali[5]:

- Contabilità del personale
- Contabilità di magazzino
- Contabilità industriale o analitica o dei costi.

L'automazione, che deriva dall'utilizzo dei sistemi informativi, permette di potenziare la capacità informativa dei dati contabili poiché consente di gestire ed effettuare elaborazioni di grandi moli di dati impossibili da trattare manualmente.
In questo modo, la contabilità generale integrata con dati statistici arriva ad avere un ruolo centrale nel sistema informativo aziendale, supportando i processi decisionali che hanno necessariamente bisogno di dati rilevati con la sistematicità e l'accuratezza tipiche della logica contabile.
I vantaggi che si ottengono con l'automazione e l'integrazione della gestione amministrativo contabile sono non soltanto efficienza in termini di risparmio economico per la riduzione del personale umano ma, soprattutto, un aumento dell'accuratezza dei dati e della tempestività di rilevazione indispensabile per il supporto decisionale.

Tuttavia, è evidente che l'affidabilità dipende strettamente dalla correttezza e dall'accuratezza dei dati immessi nel sistema informativo oltre che dalle procedure di elaborazione e gestione degli stessi.

1.2 Il rischio IT

I sistemi informativi sono strumenti indispensabili per il supporto dell'azienda ma sono anche fattore di rischio e di causa di rischi operativi che possono provocare anche

[5] Fonte D. Balducci, Tenere la contabilità, FAG, Milano, 2012.

ingenti perdite dovute ad errori di gestione, malfunzionamenti del sistema e intrusioni dall'esterno.
I sistemi informativi sono affetti da rischio IT, 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.[6]
Quindi il rischio IT è sia un rischio diretto legato al malfunzionamento della tecnologia, sia un rischio indiretto legato alle conseguenze che porterebbe ai processi operativi aziendali.
In dettaglio, nell'ambiente IT esiste una serie di rischi legata all'accesso da parte di individui a software, hardware e componenti dell'ambiente tecnologico inerenti all'uso di modifiche non autorizzate o imperfette ai programmi che possono introdurre errori o causare elaborazioni incomplete (vedi capitolo 2).

Per tale ragione, l'efficacia dei controlli intorno alle applicazioni e ai sistemi influisce direttamente sull'integrità del trattamento dei dati e sulle informazioni che sono riportate al completamento dell'elaborazione.
Le applicazioni e i sistemi hanno controlli programmati al loro interno che, se sono critici, devono essere monitorati e valutati attentamente, in particolare quando la direzione fa affidamento su di essi con una verifica dell'utente limitata o assente dei risultati dell'elaborazione.
Anche un solo errore nella gestione dei sistemi informativi sarebbe sufficiente ad esporre a perdite significative l'intera organizzazione.

Data l'importanza dell'accuratezza dell'informativa societaria, a seguito di numerosi scandali finanziari avvenuti agli inizi degli anni duemila, numerose normative, come la SOX, sono state introdotte per mitigare il rischio a tutela degli azionisti.
Non a caso quindi le nuove disposizioni dedicano ampio spazio ai principi di governo e organizzazione del sistema informativo, descrivendo anche le macrofasi di gestione del rischio ICT.
Le organizzazioni IT e di sicurezza sono state entrambe in prima linea per gli sforzi di conformità e hanno il compito in primo luogo di fornire un ambiente IT sicuro e ben

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

controllato per migliorare le prestazioni aziendali e, in secondo luogo, di assistere l'organizzazione nell'affrontare strategicamente e tatticamente i requisiti di governance, rischio e conformità.[7]

Quando si tratta di gestione della conformità, sono essenziali le capacità di mantenere e proteggere le informazioni, risolvere i problemi e fornire adeguati rapporti di conformità. Ci sono due aree da considerare:

- la conformità interna assicura il rispetto delle regole, dei regolamenti e delle best practice definite dalle politiche interne
- la conformità esterna, che è la pratica di seguire le leggi, le linee guida e i regolamenti imposti da governi, industrie e organizzazioni esterne.[8]

D'altronde la valutazione del rischio IT non è immediata e non è sempre possibile traferirlo a terzi tramite assicurazioni o esternalizzazioni.
Tuttavia, dato il grosso impatto che potrebbe avere sull'organizzazione è importante trattarlo in una prospettiva strategica, quindi controllare in maniera accurata il sistema informativo.
È necessaria una sorta di collaborazione tra le funzioni e le strutture di business che a vario titolo sono riconducibili alla tutela dei sistemi informativi al fine di sensibilizzare l'impiego della tecnologia con la consapevolezza del rischio aziendale a cui è legata.

Data la complessità del controllo la maggior parte delle grandi organizzazioni si affida ad auditor esterni che hanno il compito di[9]:

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

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

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

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

1.3 Il contesto della nascita della normativa a tutela dell'informativa finanziaria: caso Enron (USA) e caso Parmalat (Italia)

Gli inizi degli anni duemila sono stati caratterizzati da un incremento dei procedimenti giudiziari a carico delle società di revisione.

I raggiri contabili dalle stesse perpetrati, negli Stati Uniti prima e in Italia poi, nella redazione degli stati patrimoniali e dei documenti economico-finanziari delle società assistite, hanno determinato il venir meno dell'affidabilità dei revisori contabili agli occhi degli azionisti, in ordine ai compiti e alle competenze espletati.

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

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

Il caso Enron, come descritto in seguito, rappresenta poi il frutto e l'esplicitazione più evidente di tali anomali meccanismi, ma ad esso ne seguirono altri di collassi contabili, come Global Crossing (soprattutto a causa della pubblicazione sovente di bilanci pro forma basati su assunzioni e ipotesi e non su ipotesi reali), Adelphia Communications, Tyco International, Xeros Corp, Qwest Communication International, etc, tutti casi in cui si manifestava un'infedele rappresentazione delle situazioni economico, patrimoniali e finanziarie degli attori imprenditoriali coinvolti. Il punto di svolta, si è avuto con WorldCom nel giugno del 2002, in cui si era dimostrato che i manager avevano sistematicamente e per anni alterato la contabilità, per miliardi di dollari.

I tratti salienti che potevano unificare tutti questi scandali, sono comunque rappresentati da gravi irregolarità contabili e governance assolutamente debole. Molti di essi avevano come società di revisione proprio Arthur Andersen.

Questa confluenza di eventi ha gravemente danneggiato la fiducia degli investitori nella qualità delle informazioni storiche e predittive fornite dalle società pubbliche provocando il crollo della capitalizzazione di mercato di molte delle società coinvolte.

1.3.1 Caso Enron

Enron è una delle più grandi multinazionali degli Stati Uniti operante nel campo dell'energia, che tra il 1996 e il 2000 ha registrato e incrementato le vendite da 13,3 billion a 100,8 billion di dollari e nello stesso periodo ha più che raddoppiato le sue vendite dichiarate. Prima di dichiarare all'improvviso bancarotta, Enron impiegava circa 19.000 dipendenti.

Il caso Enron, verificatosi negli anni 2000, costituisce una delle ipotesi emblematiche di fallimento dei processi di revisione contabile. La società di revisione *Arthur Andersen*, a cui era stata affidata la verifica dei bilanci, in spregio a qualsiasi regola di condotta etico-professionale, aveva di fatto coperto il sistema fraudolento di bilanci truccati e scatole cinesi messo in atto da Enron allo scopo di evadere la tassazione e generare profitti gonfiati. I bilanci societari sono stati manipolati, artefatti, alterati in maniera sostanziale soprattutto grazie ad "interventi" sulle controllate estere, utilizzate per occultare i relativi debiti societari.

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

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

La cronologia della crisi vede Enron dichiarare una perdita di 1,2 billion USD nei risultati del terzo trimestre, il 16 ottobre 2001; successivamente l'Authority della concorrenza promuove un'investigazione sul caso e il 10 novembre, Dinegy,

concorrente della Enron annuncia l'acquisto di Enron per circa 7,8 billion USD, ma il progetto fallisce due settimane dopo a causa del crollo in Borsa dell'85,16%. Conseguentemente il Presidente della Commissione dell'Energia e del Commercio della Camera dei Deputati USA diede l'avvio a un'investigazione sul caso in oggetto, ed Enron finì sotto inchiesta con incluse le sue 14 controllate.

Gli illeciti adoperati da Enron furono:

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

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

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

d) Special Purpose Entities, un vero e proprio contenitore per facilitare illeciti passaggi per wash trade and contability mark-to-market, e comunque per occultare il suo indebitamento totale, oltre che gonfiare le sue attività.

1.3.2 Caso Parmalat

Parmalat fino alla fine degli anni '70, era specializzata quasi totalmente sulla produzione di latte che rappresentava l'80% del suo fatturato. Dagli anni '80 il gruppo ha intrapreso una nuova strategia di diversificazione sfruttando gli ottimi risultati ottenuti nella tecnologia, produzione, pubblicità, ampliando il suo portfolio di prodotti ai dessert, formaggi, burro besciamella, etc. Nel 1990, Parmalat Finanziaria viene quotata alla Borsa di Milano, cercando ulteriormente di espandersi nel settore alimentare, e soprattutto chiudeva numerose acquisizioni in Italia, Brasile, USA, Argentina, Uruguay e Ungheria, raggiungendo 30 Paesi nel mondo agli inizi del 2000.

Parmalat riusciva a schivare qualsiasi controllo, e in particolare, riusciva a realizzare complesse e occulte, oltre che illecite, operazioni di ingegneria finanziaria, basate

sulla falsificazione di documenti contabili, in modo anche parecchio semplice ed elementare. Sono stati utilizzati almeno 4 miliardi di euro in operazioni rischiose tramite investimenti in fondi caraibici, note di debito, azioni privilegiate, garanzie, emissioni di obbligazioni. La frode tipica, dunque, era rappresentata dalla continua falsificazione dei documenti contabili, che è durata per anni ed è stata scoperta solo a causa della mancanza di una somma davvero risibile ma necessaria, per pagare un'obbligazione in scadenza.

Gli strumenti illeciti utilizzati da Parmalat furono:

a) Acquisto e Vendita di latte in polvere, utilizzando Bonlat e Camfiled, una controllata di Singapore, grazie alle quali falsificava i contratti;

b) Contratti swap su valute estere, laddove il Gruppo utilizzava il fondo Epicurum e altre società del Gruppo per contabilizzare entrate fittizie per interesse su transazioni intersocietarie con lo scopo di ridurre il falso debito bancario con Bank of America;

c) Trasferimenti di debito intersocietario, utilizzando le controllate localizzate nei paradisi fiscali;

d) Contratti di partecipazione, come nel caso della società Buconero-Geslat che portava denaro a società sorelle mediante accordi di partecipazione, in modo tale da evitare che le esposizioni finanziarie fossero considerate un debito;

e) Fondo Epicurum, descritto da Parmalat come un investimento di liquidità in un hedge fund con attività pari a $642 million, e che poi è stato scoperto essere un fondo virtuale, con lo scopo di evitare i controlli e coprire in modo assoluto le perdite.

La cronologia della crisi inizia nel febbraio 2003, quando la società rinunciò al tentativo di collocare titoli per 500 mln di Euro a causa di condizioni sfavorevoli sul mercato e la vendita aveva sviluppato dubbi sul piano di rientro del debito esistente della società. A marzo, i responsabili dei Fondi Italiani chiesero di incontrare l'esecutivo della società per discutere dei conti. A settembre, fallì il piano di Parmalat di vendere 300 mln di Euro del debito, mentre a novembre la Consob chiede chiarimenti su 3,5 billion di liquidità e sul rimborso dei titoli in scadenza. Nello stesso mese, la società di revisione Deloitte mette in dubbio le transazioni del Fondo Epicurum nelle Isole Cayman. Nello

stesso periodo la Deutsche Bank annuncia di possedere più del 5% delle quote Parmalat. La situazione si aggravò a dicembre quando Parmalat non rimborsò il pagamento di un bond per 150 mln di Euro e gli scambi sul mercato borsistico furono sospesi per tre giorni, segnando un crollo delle azioni del 47,4% e la conseguente dimissione di Calisto Tanzi, maggiore azionista della società e Capo Esecutivo della stessa. Il maggiore crollo fu quando la Bank of America scoprì un documento che presentava 3,9 billion di Euro nella contabilità bancaria della Bonlats contraffatto e i valori di quotazione delle azioni precipitò di oltre il 95%. Seguì un'inchiesta per frode, avviata dal Primo Ministro del Governo Italiano, al fine di tutelare i lavoratori. Parmalat fu sospesa dalla Borsa e sottoposta ad Amministrazione straordinaria, estesa a tutte le società del gruppo.

In entrambi i casi descritti sopra, erano presenti chiarissime irregolarità e illiceità che violavano i principi di revisione standard. Da quanto descritto, si può notare come fosse presente una debolezza strutturale negli organi deputati al controllo interno.[10]

1.4 SOX

Di fronte a tale situazione critica che investiva gran parte del panorama imprenditoriale americano, che trovava i suoi elementi di debolezza, non solo in politiche malverse e fraudolente da parte dei vertici aziendali e delle società di revisione la politica americana è stata solerte e fortemente reattiva. Il risultato è rappresentato, infatti, dal Sarbanes-OxleyAct, che ha rivoluzionato il concetto di trasparenza nell'informativa contabile, e consolidato massimamente gli strumenti di contrasto delle frodi societarie e contabili.

La Sarbanes-Oxley Act, meglio conosciuta come SOX, è una normativa istituita nel 2002 negli USA a seguito degli scandali finanziari Enron e WorldCom, ponendosi come obiettivo il ripristino della fiducia degli investitori e la protezione degli azionisti. La SOX è stata introdotta per garantire la trasparenza della contabilità generale, ovvero ridurre le possibilità di frodi, e per migliorare la corporate governance. In

[10] Mirko Alchirafi, tesi di laurea, 2011, *INDIPENDENZA E CONFLITTO D'INTERESSI NELLA REVISIONE LEGALE DEI CONTI: QUALITA' ED EVOLUZIONE DELLE FUNZIONI DEL REVISORE ALLA LUCE DELLE RECENTI RIFORME*

particolare, la Sarbanes-Oxley si concentra sul ruolo critico del "controllo interno" ed affida, esplicitamente ai CEO e ai CFO la responsabilità di stabilire, valutare e monitorare l'efficacia del controllo interno sull'informativa finanziaria.[11]

La criticità che mira a risolvere la SOX è lo scollamento tra i consigli di amministrazione che hanno la responsabilità finale per un controllo interno efficace e quei dipendenti che devono svolgere le attività di controllo. La SOX ha l'intento quindi di collegare le attività di controllo a livello operativo con le attività di governance a livello di consiglio di amministrazione.

L'efficacia dei programmi di preparazione e di conformità dovrebbe colmare tale lacuna.

Per un'azienda pubblica, la conformità ai requisiti Sarbanes-Oxley non è negoziabile, infatti, con l'introduzione della normativa è stata creata la *Public Company Accounting Oversight Board* (PCAOB), società senza scopo di lucro, che ha il compito di sorvegliare sull'applicazione dei principi contabili SOX. La supervisione, a sua volta, della Public Company Accounting Oversight Board è invece a cura della SEC, *Securities and Exchange Commission* (Commissione per i Titoli e gli Scambi), l'agenzia federale statunitense preposta alla vigilanza della borsa valori.[12]

La normativa SOX si applica a tutte le entità che hanno una classe di titoli registrata ai sensi della Sezione 12 dello Exchange Act, o che sono tenute a presentare rapporti ai sensi della Sezione 15 (d) del Securities Exchange Act del 1934.
Nello specifico, la SOX si applica a tutte le società americane e alle società di diritto estero quotate al NYSE (New York Stock Exchange).
In particolare, come mostrato in Figura le società quotate al NYSE sono interessate principalmente alle sezioni della normativa sulla:

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

[11] Sarbanes-Oxley Act Guideline, eaca European Association of Communications Agencies, https://www.eaca.eu/wp-content/uploads/2016/06/sarbanes.pdf
[12] *Qual è il Public Company Accounting Oversight Board?* Gennaio 2013, snowviewfarm.com, https://www.snowviewfarm.com/qual-e-il-public-company-accounting-oversight-board/

	Section 302	Section 404	Section 906
When is it effective?	August 29, 2002	Fiscal years ended on or after: • November 15, 2004, for U.S. accelerated filers* • July 15, 2006, for foreign accelerated filers* • December 15, 2007, for others	July 30, 2002
Who signs off?	• CEO • CFO	• Management • Independent accountant	• CEO • CFO
What's it about?	• Executive certification issued quarterly	• Internal control report annually • Independent accountant attests to annual report • Quarterly review for change	• Abbreviated certification issued quarterly • Criminal penalties
How often are the evaluations?	• Quarterly evaluation	• Annual assessment • Quarterly review for change	• Quarterly evaluation

Figure 1.1 GUIDE TO THE SARBANES-OXLEY ACT: Internal Control Reporting Requirements (Fourth Edition), protiviti

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

La novità introdotta da questa sezione è proprio l'imposizione, in capo a questi ultimi, di un obbligo di certificazione dei bilanci che attesti che hanno effettuato una valutazione della progettazione e dell'efficacia di tali controlli al fine di migliorare l'informativa finanziaria. A maggiore supporto di tale obiettivo, i responsabili della certificazione devono dichiarare di aver comunicato al loro comitato di revisione contabile e al revisore indipendente eventuali carenze significative nei controlli, debolezze rilevanti e atti di frode. La SEC ha inoltre proposto un requisito di certificazione ampliato che include i controlli interni e le procedure per l'informativa finanziaria, oltre al requisito relativo ai controlli e alle procedure di divulgazione.

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

- sono responsabili dei controlli e delle procedure di comunicazione;
- hanno progettato (o supervisionato la progettazione di tali controlli) al fine di assicurare che le informazioni rilevanti siano loro rese note;
- hanno valutato l'efficacia di tali controlli con cadenza trimestrale;
- hanno presentato le loro conclusioni in merito all'efficacia di tali controlli;
- hanno comunicato al loro comitato per il controllo interno e alla società di revisione contabile eventuali carenze significative dei controlli, carenze rilevanti e frodi che coinvolgono il management o altri dipendenti che hanno un ruolo determinante nel controllo interno della società;
- hanno indicato nel deposito eventuali modifiche significative dei controlli. [13]

La certificazione dell'**articolo 906**, è una dichiarazione più breve, in cui è richiesto al CEO e ai CFO di firmare e certificare la relazione periodica contenente i rendiconti finanziari. La suddetta certificazione esecutiva deve affermare che la relazione è conforme ai requisiti di reporting della SEC e rappresentare correttamente la condizione finanziaria dell'azienda e i risultati delle sue operazioni. Il mancato rispetto di questo requisito comporta multe fino a 5 milioni di dollari e può essere imposta la reclusione fino a 20 anni per non conformità consapevole o intenzionale. [14]

Entrambe le serie di requisiti di certificazione di cui alle sezioni 302 e 906 sono necessarie, anche se si sovrappongono in modo significativo. Tuttavia, una certificazione fraudolenta della sezione 302 è soggetta all'applicazione civile da parte della Commissione, mentre una certificazione fraudolenta della sezione 906 comporta sanzioni penali applicabili dal Dipartimento di giustizia. [15]

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

[13] *SOX Section 302: Corporate Responsibility for Financial Reports*, Sarbanes Oxley, https://www.sarbanes-oxley-101.com/SOX-302.htm
[14] *SOX Section 906: Corporate Responsibility for Financial Reports*, Sarbanes Oxley, https://www.sarbanes-oxley-101.com/SOX-906.htm
[15] GUIDE TO THE SARBANES-OXLEY ACT: Internal Control Reporting Requirements (Fourth Edition), protiviti

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

- afferma di essere responsabile dell'istituzione e del mantenimento dei controlli interni e delle procedure di informativa finanziaria;
- valuta e giunge a conclusioni sull'efficacia dei controlli interni e delle procedure di informativa finanziaria;
- dichiara che la società di revisione contabile ha attestato e riferito in merito alla valutazione, da parte del management, dei controlli interni e delle procedure di informativa finanziaria della società, seguendo gli standard istituiti dal PCAOB. [16]

Poiché il CEO e il CFO dell'azienda devono rilasciare dichiarazioni pubbliche sull'efficacia del controllo interno, è necessario che il management mantenga un supporto sostanziale e una documentazione riguardante sia la struttura di controllo interno che la propria valutazione.

Gli auditor esterni devono attestare, redigendo una relazione separata, l'efficacia del controllo interno della società e l'affermazione del management sull'efficacia dei controlli interni e delle procedure per l'informativa finanziaria. Il rapporto da redigere deve contenere [17]:

- Dettagli su come il management gestisce e mantiene un adeguato sistema di controllo interno sulla rendicontazione finanziaria supportato da idonee evidenze
- Dettagli sul framework, che deve essere un modello di controllo idoneo e riconosciuto, utilizzato dal management per la valutazione dei controlli interni, al fine di fornire criteri ai valutatori sull'efficacia del sistema
- Descrizione completa degli obiettivi di controllo creati dal management per affrontare i rischi identificati e le relative attività di controllo;

16 *SOX Section 404: Management Assessment of Internal Controls*, Sarbanes Oxley, https://www.sarbanes-oxley-101.com/SOX-404.htm

17 *SOX Compliance Requirement & Overview*, 15 Gennaio 2020, AUDITBOARD, https://www.auditboard.com/sox-compliance/

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

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

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

La valutazione dell'esistenza di una condizione da segnalare è un processo soggettivo che dipende da fattori quali la natura del sistema contabile, l'importo di bilancio, l'ambiente generale di controllo e il giudizio di coloro che prendono la decisione. La presenza di una o più carenze rilevanti può indicare che la struttura di controllo interno non è efficace.

Gli attori principali coinvolti dalla normativa sono dunque il consiglio di amministrazione, che supervisiona l'impegno dell'azienda nel rispettare i compiti di cui sopra; il CEO e il CFO, che hanno la responsabilità di garantire la conformità e comunicano queste informazioni al management e ai dipendenti chiave; il comitato

direttivo, che supervisiona e coordina le attività Sarbanes-Oxley in tutta l'organizzazione.

Nelle aziende più piccole, il comitato direttivo può essere composto solo da due persone che certificano l'efficacia del controllo interno - il CEO e il CFO. Nelle organizzazioni più grandi, i membri possono includere altri dirigenti, come il direttore contabile, il direttore della revisione interna e il consulente generale, nonché un consulente del comitato di revisione contabile.

Nelle aziende di tutte le dimensioni, dovrebbe essere vassegnato un amministratore designato dal consiglio di amministrazione per monitorare i processi e i progressi del comitato direttivo. Le funzioni del comitato direttivo includono:

- stabilire i parametri in base ai quali opererà il comitato di divulgazione;

- identificare le persone necessarie per raggiungere gli obiettivi;

-tenere informati il consiglio di amministrazione e la direzione dei progressi compiuti.

1.4.1 Fasi di un progetto SOX

La guida SEC spiega che il "rischio" comprende sia il rischio di errori materiali o frodi sia il rischio di fallimento del controllo. Per la valutazione sul sistema di controllo interno, il management deve istituire il *Management Assessment Process*, un processo strutturato, in cui, per quanto detto sopra:

- Il management dovrebbe valutare la progettazione (design) dei controlli che ha implementato per determinare se esiste una ragionevole possibilità che un errore significativo nel bilancio non possa essere prevenuto o rilevato in modo tempestivo
- Il management dovrebbe raccogliere e analizzare le prove del funzionamento (operation) dei controlli oggetto di valutazione in base alla sua valutazione del rischio associato a tali controlli.

Di conseguenza il management applica un approccio top-down, basato sul rischio, che promuove l'efficienza focalizzandosi solo su quei "controlli chiave" necessari per prevenire o rilevare errori significativi nel bilancio e cerca di allineare la natura e

l'estensione delle procedure di valutazione con quelle aree di rendicontazione finanziaria che presentano il rischio maggiore di fallimento del controllo. Il *Management Assessment Process*, per rispettare i requisiti del Public Company Accounting Oversight Board, deve coprire un certo numero di attività.

Le macro attività coinvolte sono il Process Mapping, l'Assessment e il Remediation & Reporting come mostrato in Figura.

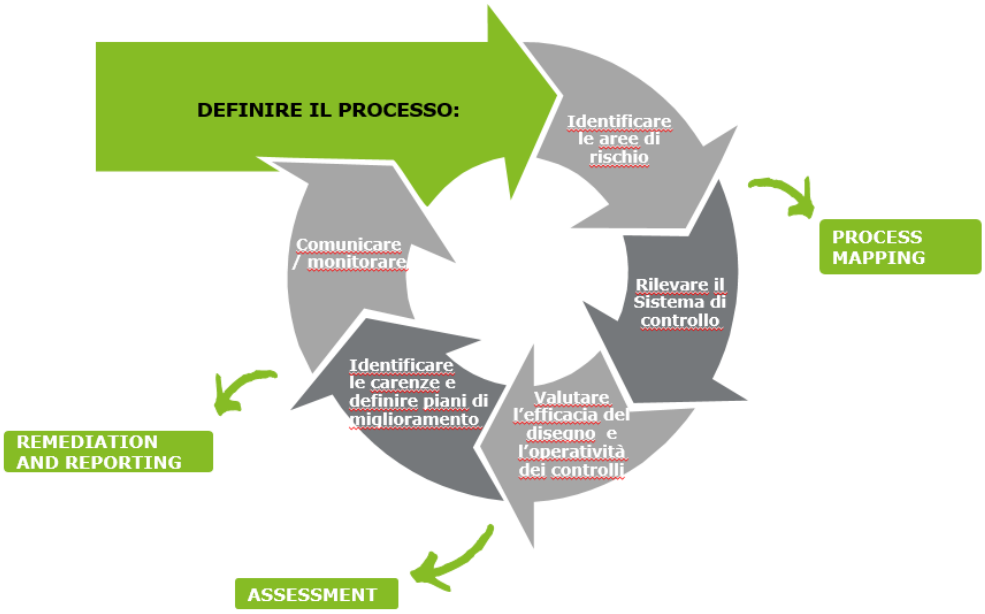


Figure 1.2 Management Assessment Process, Deloitte

- Effettuare Process Mapping (Figura) comporta catalogare i processi di business in modo da identificare il loro impatto finanziario e mappare i rischi annessi a ciascuno di essi, così da associare un controllo ad ogni rischio individuato. Gli strumenti utilizzati per realizzare la mappatura sono le Narrative e la Risk Control Matrix.

  - Le Narrative sono documenti in cui si descrivono i processi con i principali attori e responsabilità e le loro relative modalità operative e di controllo.

- La Risk Control Matrix (RCM) è una matrice in cui si identifica e si valuta ciascuna attività di controllo.

In questa fase si procede a legare a ciascun processo le rispettive voci di bilancio e ad associargli un livello di rischio in base alla rilevanza di esse. Il rischio è assegnato tenendo conto della probabilità di passività potenziali e della complessità della contabilità e del reporting. Il management ha il compito di individuare controlli specifici per mitigare il rischio di frode, e quindi, di progettare programmi specifici per prevenirlo.

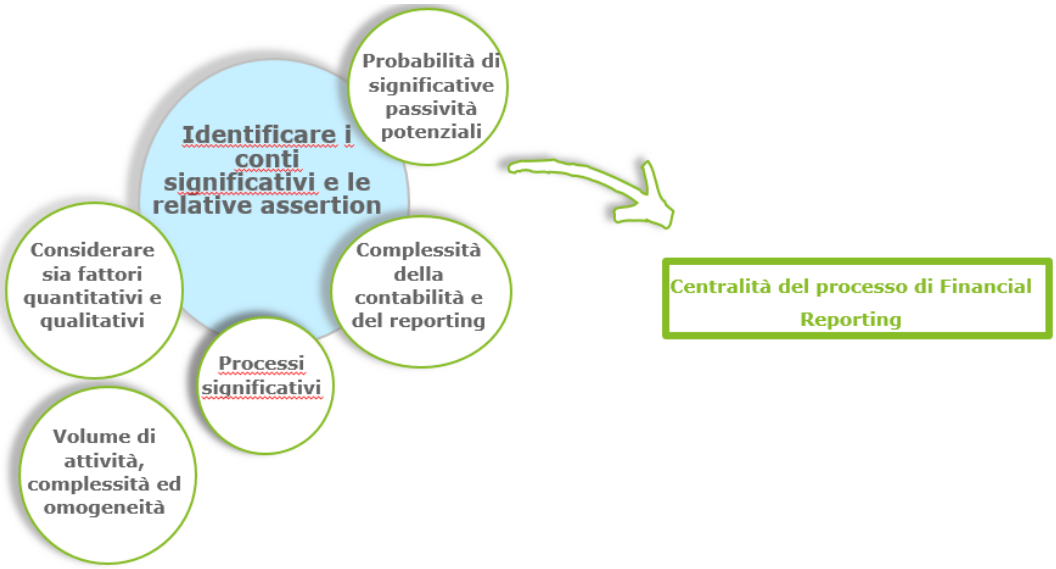


Figure 1.3 Fasi di un processo SOX, Process Mapping; Deloitte

- Fare Assessment implica valutare il *design effectiveness* e valutare l'*operating effectiveness* ovvero l'efficacia del disegno dei controlli e l'operatività degli stessi, con l'obiettivo di scoprire le carenze dell'SCI, Sistema di Controllo Interno. Per l'assessment viene utilizzato un framework specifico che sarà trattato nel secondo capitolo.
- Fare Remediation comporta organizzare piani di remediation ad eventuali criticità scoperte e attuare un sistema di monitoring per mitigarle. Con il

reporting si richiede l'attestazione del Management sulla situazione individuata, come mostrato in Figura. [18]

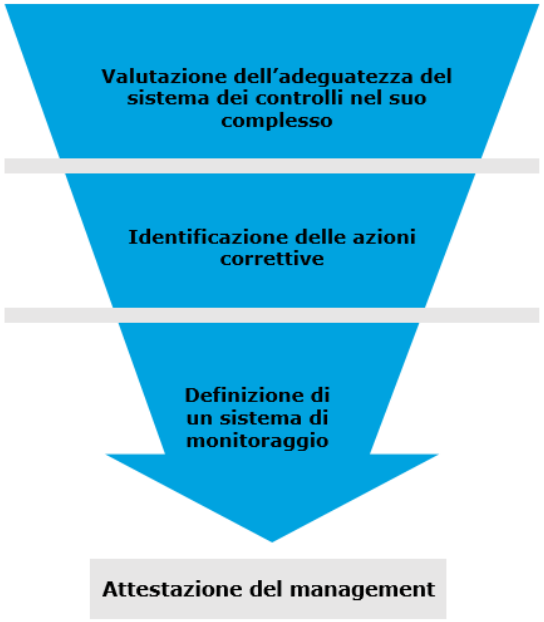


Figure 1.2 Fasi di un processo SOX, Remediation and Reporting; Deloitte

Una forte struttura di controllo interno può aiutare l'azienda a:

- prendere decisioni aziendali migliori con informazioni di maggiore qualità e tempestività;
- guadagnare (o riconquistare) la fiducia degli investitori;
- prevenire la perdita di risorse;
- rispettare le leggi e i regolamenti applicabili;
- ottenere un vantaggio competitivo attraverso operazioni semplificate.

Al contrario, le conseguenze di un fallimento potrebbero essere a dir poco disastrose. Le aziende che trascurano di istituire i controlli necessari possono trovarsi in situazioni simili a quelle che hanno portato alla promulgazione di Sarbanes-Oxley, con conseguente:

[18] Source Portale Deloitte, Tech Library

- aumento dell'esposizione alle frodi;
- sanzioni da parte della SEC;
- pubblicità sfavorevole;
- impatto negativo sul valore dell'azionista;
- azioni legali.

L'obiettivo che si vuole ottenere con la SOX è quello di rendere l'azienda leader riconosciuto nella governance aziendale, essendo quindi nota per la qualità e l'integrità del reporting finanziario, in modo da avere un migliore flusso di informazioni per prendere decisioni commerciali migliori.

1.5 Legge italiana

L'adeguamento alla SOX è richiesto alle società italiane quotate in USA oppure alle società che sono controllate da gruppi quotati in USA. Il legislatore italiano, è stato di conseguenza indotto a inserire una nuova normativa nella legislazione nazionale, la *Legge sul risparmio*, (legge 28 dicembre 2005, n. 262) con l'intento di migliorare l'informativa finanziaria delle società quotate.

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

In particolare, l'articolo 154-bis, il primo della sezione V bis del D.Lgs. n. 58/98 TUF, tratta sulla redazione dei documenti contabili societari e prevede la nomina di un dirigente, scelto dall'organo di controllo aziendale, che è preposto alla redazione degli stessi. Costui ha il compito di scrivere una dichiarazione, insieme al direttore generale, che attesti sulla veridicità della situazione economica, patrimoniale e finanziaria della società al fine di certificare gli atti e le comunicazioni diffuse sul mercato e previste dalla legge.[19]

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

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

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

Il dirigente preposto deve anche predisporre procedure amministrative e contabili per ogni comunicazione di carattere finanziario e per la redazione del bilancio d'esercizio e del bilancio consolidato. Ne deriva che, al fine di rispettare questi compiti assegnatigli, il preposto deve avere adeguati poteri e mezzi per ricavare le informazioni. [20]

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

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

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

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

Esso prevede che l'ente risponda se le persone appartenenti ad esso hanno agito nell'interesse di esso o a suo vantaggio e non solo nell'interesse esclusivo proprio o di terzi. Le persone considerate sono coloro che svolgono funzioni di rappresentanza, di direzione, di amministrazione, coloro che esercitano la gestione e il controllo anche di fatto o persone sottoposte alla vigilanza o alla direzione di uno di loro. L'ente è esonerato dalla responsabilità se l'organo dirigente ha adottato modelli gestione e di organizzazione idonei a prevenire i reati, non trascurando di applicare un'attenta vigilanza, dunque, le persone che hanno commesso il reato hanno eluso in modo fraudolento i modelli stessi.

La legge richiede che per attuare in modo efficace un modello di organizzazione, vi sia un sistema sanzionatorio idoneo per il mancato rispetto delle misure, ma anche una verifica periodica di esso affinché sia sempre allineato ad eventuali mutamenti dell'organizzazione. [21]

1.6 Controllore e controllato

La revisione esterna della contabilità nasce dall'esigenza degli azionisti di far verificare da un'entità indipendente, data la grande asimmetria informativa, se quanto riportato nel bilancio dell'azienda interessata corrisponda al vero.

Infatti, un sistema di controllo interno effettuato dalle sole aziende non è sufficiente poiché si generano problemi di monitoraggio e incentivazione in merito alle informazioni contabili, potendo queste ultime essere manipolate e modificate per scopi ulteriori e diversi rispetto al controllo stesso. Se il controllo fosse effettuato solo internamente, i manager potrebbero mentire, in maniera fraudolenta, sulle reali prospettive della società, occultando le criticità gestionali, economiche e finanziarie, semplicemente falsando i bilanci.

Per queste ragioni controllore e controllato non possono appartenere alla stessa società e si deve ricorrere a una revisione esterna con un rapporto di agenzia.

La società di consulenza esterna (agente), sotto un adeguato sistema di incentivi, ha il compito di revisionare il sistema di controllo interno della società (principale). Di nuovo si genera, però, il problema di chi controlla il controllore.

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

Di conseguenza, alla luce degli scandali Enron e Worldcom, poiché si era persa la fiducia nell'operato delle società di revisione, è stato istituito il PCAOB, società senza scopo di lucro, che ha il compito di sorvegliare sull'applicazione dei principi contabili SOX.

Alla luce di quanto esposto le aziende devono disporre di un framework di riferimento e di una governance adeguati, per diagnosticare e affrontare i rischi etici e di conformità, e per garantire che l'azienda e i suoi partner possano gestire tali rischi in modo completo ed economico. In caso contrario, possono dover affrontare azioni normative, multe e perdite di reputazione. [22]

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

CAPITOLO 2

A seguito degli scandali Enron e Parmalat, i controlli interni sono diventati sempre più importanti. Un sistema di controllo interno efficace è un requisito del Sarbanes- Oxley Act del 2002 che regola il reporting e la verifica dei controlli interni sul reporting finanziario per le società pubbliche.

I controlli interni svolgono un ruolo critico non solo nelle aziende pubbliche ma anche in quelle private, poiché tutelano i beni di un'organizzazione e riducono le possibilità che la società commetta frodi e che gli errori non vengano rilevati nelle operazioni quotidiane di un'organizzazione.

Ma perché è così importante effettuare un controllo interno?[23]

1. I Controlli Interni aiutano a comprendere e a mitigare i rischi.
   Sono infatti stabiliti sulla base di un approccio orientato al rischio. Comprendere i rischi permette di determinare se ci sono controlli adeguati per mitigarli.
2. I Controlli Interni aiutano a verificare le asserzioni di bilancio in termini di esistenza, diritti, completezza e accuratezza.
3. I Controlli Interni aiutano a prevenire e rilevare le frodi attraverso la separazione dei compiti (SOD), metodo per gestire i conflitti di interesse.
4. I controlli interni aiutano a prevenire le inesattezze nel bilancio.
5. I controlli interni aiutano a documentare le pratiche aziendali. Se non si dispone di prove documentali dei controlli interni, non è possibile dimostrare l'esistenza di essi.

[23] Emma Zhang, 1 Giugno 2016, *The importance of Internal Controls in Accounting,* Carrtegra, http://www.carrtegra.com/2016/06/importance-internal-controls-accounting/

2.1 Il Sistema di controllo interno

I controlli interni sono i meccanismi, le regole e le procedure attuate da una società per garantire l'integrità delle informazioni finanziarie e contabili, promuovere la responsabilità e prevenire le frodi. Essi possono contribuire ad accrescere l'efficienza operativa migliorando l'accuratezza e la tempestività della rendicontazione finanziaria oltre a supportare la compliance. [24]

In merito a quest'ultima, per la sezione 404 della SOX, le società devono detenere un sistema di controllo interno e sono obbligate a riferire in merito alla valutazione di esso da parte delle società di revisione contabile le quali devono rispettare, nel loro operato, gli standard PCAOB.

Il parere del revisore contabile (auditor) che accompagna i rendiconti finanziari si basa su una revisione delle procedure e delle registrazioni utilizzate per produrli. Nell'ambito di una revisione, i revisori esterni verificano i processi contabili e i controlli interni della società e forniscono un parere sulla loro efficacia.

Tuttavia, indipendentemente dalle politiche e dalle procedure stabilite da un'organizzazione, è possibile fornire solo una ragionevole garanzia che i controlli interni siano efficaci e che le informazioni finanziarie siano corrette. L'efficacia dei controlli interni testata dalla società e dall'audit è limitata dal giudizio umano.

2.2 Internal Control Integrated Framework: COSO FRAMEWORK

La conformità al Sarbanes-Oxley Act non crea un ambiente privo di rischi, che di fatto non esiste. Tuttavia, conformarsi ad esso ed avere una corretta governance dell'IT aiuta ad ottenere report finanziari più tempestivi ed accurati.[25]

L'adeguatezza del sistema di controllo interno e di gestione dei rischi è fondamentale ai sensi del D.Lgs. 231/01 pena la responsabilità primaria del Consiglio di Amministrazione. L'adeguatezza è la capacità di gestione di tutti i rischi che si presentano nel tempo, ovvero il sistema di controlli adottato e la solidità dei processi aziendali.

[24] Will Kenton, 25 giugno 2019, *Internal Controls,* Investopedia
https://www.investopedia.com/terms/i/internalcontrols.asp
[25] *Obiettivi di controllo IT per il Sarbanes_Oxley Acr*, 2° Edizione, settembre 2016

Essendo la gestione e valutazione continua del sistema di controllo interno complessa, le imprese fanno riferimento a framework standard, specialmente per salvaguardare il rischio IT. Il framework più diffuso e utilizzato è Il "*COSO Framework".*

Tra i suoi obiettivi vi sono fornire un modello di riferimento comune che possa essere valutato in modo univoco dalle diverse parti interessate e stabilire una definizione di sistema di controllo interno.

Secondo 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".*

A detta del framework per ottenere un adeguato Sistema di Controllo Interno è necessario svolgere cinque operazioni fondamentali che costituiscono il Ciclo di Audit.[26]

- *Control Environment*. L'organizzazione deve avere un codice etico e di integrità, un sistema sanzionatorio e politiche di incentivazione.
  Il consiglio di amministrazione deve essere indipendente rispetto al management e deve supervisionare il sistema di controllo interno redigendo relazioni sulla Corporate Governance, Policy di Enterprise Risk Management e piani di Internal Audit risk based.

- *Risk Assessment*. L'organizzazione deve identificare i rischi e le frodi legati agli obiettivi aziendali e valutare come gestirli, quindi implementare piani di monitoraggio dei Key Risk Indicator, strumenti di Governance Risk e Compliance (GRC), Analisi SWOT e dei competitor.

- *Control Activities*. L'organizzazione deve implementare attività di controllo per ridurre i rischi entro livelli accettabili predisponendo documenti di Gap Analysis e la lista dei principi di SoD con il dettaglio delle job description.
  Inoltre, l'organizzazione deve implementare attività di controllo sulla tecnologia quali:

[26] ASSIREVI, Gennaio 2019, Monografia COSO Framework

- Mappatura degli applicativi aziendali
- Verifiche del disegno e dell'operatività dei controlli
  - Test dei GITC (General Information Technology Controls)
    1. User Access Management
    2. Change Management
  - Test dei controlli automatici (ITAC)

- *Information & Communication*. L'organizzazione deve comunicare esternamente le relazioni annuali e periodiche ed internamente gli obiettivi del Sistema di Controllo Interno e i risultati del Risk Assessment. Inoltre, deve generare informazioni utili con sistemi contabili, gestionali e di business intelligence.

- *Monitoring*. L'organizzazione deve valutare continuamente il funzionamento del sistema di controllo interno, applicando certificazioni ISO per la qualità e controllando la produzione, l'ageing del credito e le azioni correttive.

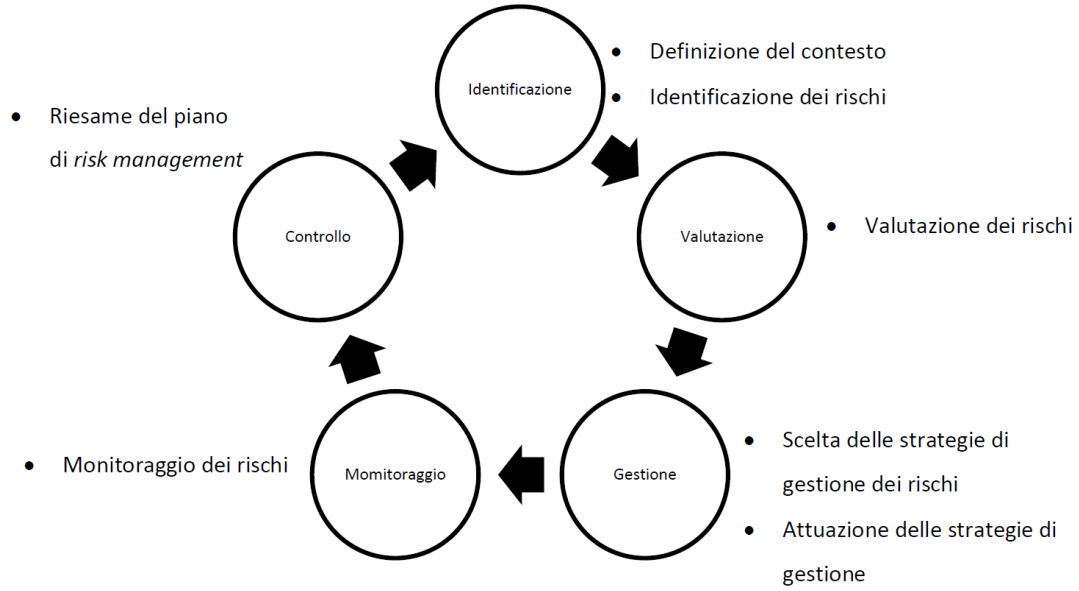


Figura 2.1

Un'azienda dovrebbe possedere competenze di controllo relativamente all'IT per tutti i cinque elementi COSO individuati come essenziali per un controllo interno efficace.

Nella seguente Figura è mostrato come riuscire ad ottenere un elevato valore di business in funzione della conformità alla SOX. Il valore è crescente con l'operare dei seguenti step:

1. Pianificare e definire il perimetro dei controlli IT
2. Valutare i rischi
3. Documentare i controlli: GITC, ITAC, IPE
4. Valutare il disegno dei controlli e l'efficacia operativa
5. Valutare le priorità e risolvere le carenze
6. Costruire la sostenibilità

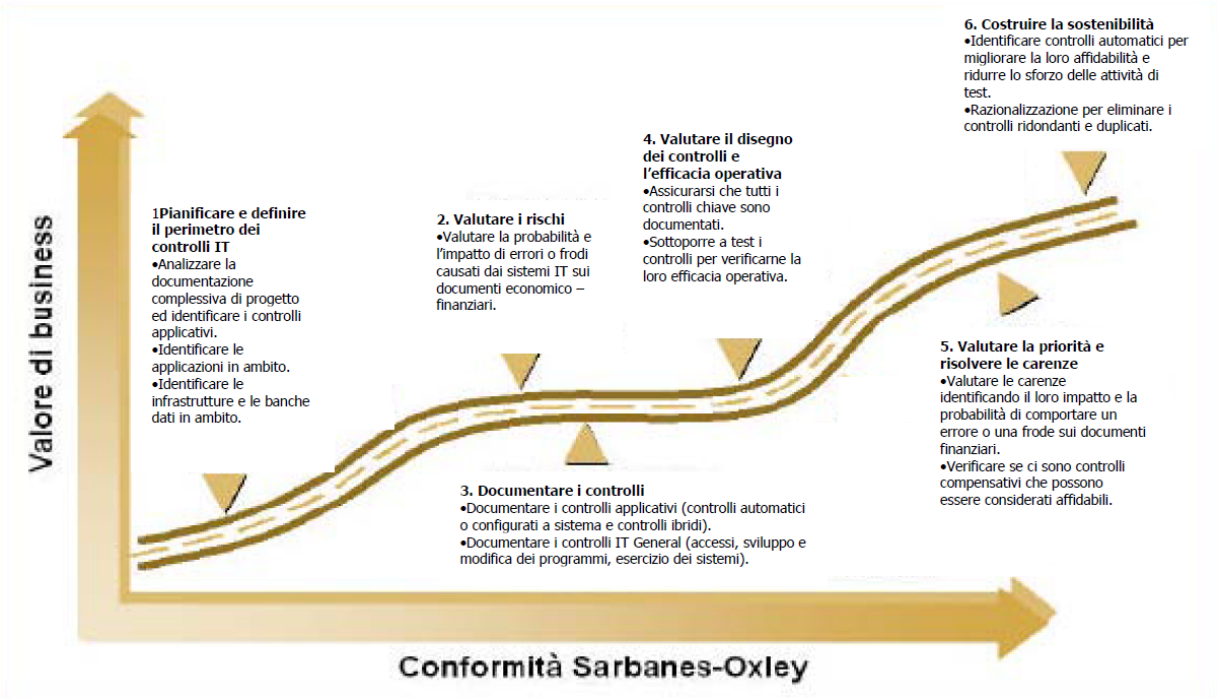


Figure 2.2 Mappa per la conformità IT, Obiettivi di controllo IT per il Sarbanes_Oxley Act, 2° Edizione, settembre 2016

2.3 L'attività di Supporto Audit (IT Specialist)

L'auditing è definita come l'attività di verifica in loco di un processo o di un sistema di qualità, per garantire la conformità ai requisiti normativi. L'audit può operare a supporto di un'intera organizzazione o può essere specifico per una funzione, un processo o una fase di produzione.[27]

L'IS Audit o IT Audit, opera in veste di supporto all'Audit, in quanto eroga un servizio di auditing tecnologico che si incentra sull'Information Security.

Mediante la valutazione dei rischi connessi alla gestione dei sistemi IT, l'IT audit fornisce valutazioni di adeguatezza e robustezza dei sistemi informativi a supporto dei processi fiscali e contabili ed indica mirati piani di miglioramento per aumentare l'efficacia e la robustezza dei sistemi IT. [28]

Le attività di IT Audit costituiscono un sottoinsieme delle attività complessive di revisione contabile del bilancio e sono declinate in subordine alla natura e all'incarico a cui queste ultime si uniformano.

La metodologia dell'IT Audit prevede di andare ad analizzare l'ambiente IT (applicativi, database, OS) ed assegnargli un livello di rischio, poi di andare a mappare i controlli effettuati sul sistema IT in base ai rischi rilevanti che dovrebbero coprire, testarne design e operative effectiveness (GITC, IPE, IUC, ITAC), valutare le deficiency e come mitigarle.

I controlli effettuati dall'IT Audit coinvolgono:

- Applicativi, ovvero tutti quei sistemi contabili e gestionali utilizzati dalle società per lo svolgimento dei processi di business. Esempi di sistemi gestionali sono SAP, Hyperion, Navision e AS400;
- Database (DB) ovvero gli archivi informatici di dati come SQL, Oracle, DB2 e Hana.

[27] https://asq.org/quality-resources/auditing

[28] IS Audit & Compliance Support, https://www.bdo.it/it-it/services-it/advisory/digital-consulting/is-audit-compliance-support

- Sistemi operativi (OS) ovvero i programmi che gestiscono in contemporanea tutti gli applicativi adoperati dalla società. Esempi di OS sono Windows, UNIX e AS400

L'ultimo tassello importante della metodologia audit è la valutazione della quantità di lavoro necessario, inclusa la necessità di competenze specialistiche. Dato che la tempistica e la disponibilità di risorse umane adeguate per l'audit IT rappresentano di solito una sfida, fare questo passo in modo corretto dovrebbe tradursi in un lavoro di audit di qualità più elevata e a costi inferiori.

2.3.1 Pianificare e definire il perimetro dei controlli IT

Durante la fase di pianificazione è importante considerare l'adeguatezza e l'efficacia dei sistemi di controllo in relazione ad un adeguato modello (Coso,ecc).

La pianificazione dell'incarico risulta di vitale importanza in quanto:

- Permette di individuare gli obiettivi che l'IT Audit, di comune accordo con l'Audit, intende perseguire e che si traducono in una valutazione preliminare dei rischi dell'attività che saranno oggetto di revisione (General IT Controls);
- Delimita l'ambito dell'audit in termini temporali e materiali dell'analisi interna;
- Permette una programmazione del lavoro (audit program) ossia identificare, esaminare, stimare e documentare le informazioni raccolte durante l'esecuzione dello stesso;
- Permette una prima definizione di risorse umane finanziarie ed informatiche necessarie per lo svolgimento dell'analisi.

IT Planning Memo

Le attività di IT Audit devono presentare una logica rigorosa di svolgimento delle attività di pianificazione e per questa ragione la metodologia richiede che esse siano definite da un puntuale IT Planning Memo. Per la specifica competenza tecnica necessaria al loro svolgimento il planning memo delle attività di IT Audit deve essere predisposto dal team di IT Specialist coinvolto nella loro pianificazione.

L'IT Audit Planning Memo è il prodotto finale della categoria di procedure "IT Understanding and Audit Planning" e si articola in vari paragrafi raggruppabili nei seguenti argomenti:

- Macro mappatura degli ambienti IT dell'azienda, in termini di: Sistemi operativi e software di base, Hardware e ubicazione dello stesso, Processi IT, organizzazione e risorse umane
- Comprensione del sistema informativo rilevante per il bilancio
    - Applicativi del Cliente rilevanti per l'audit
    - Infrastrutture degli applicativi rilevanti
    - Se applicabile, evaluation of Service organization controls

- Identificazione e valutazione dei rischi, ivi inclusi quelli relativi all'elaborazione dei dati
- Configurazione dei test dei controlli e del relativo piano
- Svolgimento dei test dei controlli
- Attività di Roll forward
- Deficiency evaluation e materialità
- Stima budget necessario per lo svolgimento delle attività

Dati i contenuti, l'ITSPM (IT Specialist Planning Memo) presuppone un'attività organica di comprensione dei sistemi IT del Cliente che determinano scritture contabili. L'attività anzidetta è finalizzata ad identificare gli applicativi che producono eventi contabili e che concorrono alle relative registrazioni e attengono a conti di bilancio o classi di transazioni per i quali l'Audit team ha optato per una strategia di Operating Effectiveness (OE) reliance.

Si richiama l'attenzione sul fatto che l'IT Audit Planning Memo determina la giustificazione delle attività di IT Audit sia sotto il profilo della integrazione e declinazione di queste nelle procedure previste per tutta l'attività di revisione del bilancio (dedotta dall'Audit Planning Memo), sia sotto il profilo della loro accurata e completa esecuzione, che saranno attestate a fine lavoro dall'IT Specialist Summary memo.

Understanding of IT Environment

Oltre al Planning Memo l'IT Specialist redige anche un documento chiamato *Understanding of IT Environment*.

Un ambiente IT può essere definito come le politiche e le procedure che un'entità implementa e i sistemi applicativi, gli autori di report e l'infrastruttura IT sottostante (database, sistemi operativi, reti, interfacce, middleware) che l'entità utilizza per supportare le operazioni di business e realizzare le strategie di business.

In tale ambito sono rilevati l'organizzazione IT e le principali attività in essere a supporto dei processi IT, con riferimento anche alle aree di General IT Controls che sono:

- Data center e Network Operations

- Sicurezza degli accessi
- Acquisizione, sviluppo e modifica dei sistemi software applicativi
- Acquisizione, modifica e manutenzione dei sistemi software di base
- Modifiche ai programmi di elaborazione dati

In particolare, si effettua:

- Un'analisi dell'Organizzazione attuale dell'Area ICT e la valutazione di possibili sviluppi futuri a livello organizzativo in un'ottica di miglioramento delle performance del Servizio IT in termini sia di efficacia che di efficienza.
- Un'analisi a livello macro dei principali progetti in corso e/o già approvati al fine di comprenderne le eventuali implicazioni dirette o indirette sull'Area ICT, con relativa analisi di quali potrebbero essere gli eventuali impatti sui processi di business aziendali e sui SI stessi.
- Una valutazione a livello macro delle modifiche eseguite dalla Società sull'infrastruttura tecnologica (HW) e applicativa (SW) ed analisi dei conseguenti cambiamenti in termini di flussi d'informazioni e dati tra gli applicativi

La rilevazione è finalizzata all'identificazione di eventuali IT risks.

2.3.2. Valutare i rischi

Una valutazione del rischio IT è una revisione completa dell'organizzazione IT della società, con l'obiettivo di identificare le criticità esistenti che potrebbero essere sfruttate per minacciare la sicurezza della rete e dei dati. Serve come base per decidere quali eventuali contromisure adottare per ridurre il rischio a un livello accettabile, sulla base del valore della risorsa informativa per l'organizzazione.

All'interno di un ciclo di business è possibile identificare tre tipologie di rischio su tre livelli diversi:

- Risks of Material Missastement (RoMMs): rischio a livello del ciclo di business. Tali rischi sono solitamente identificati dal team di Audit.
- Risks Arising from IT (RAITs): rischio a livello di applicativo. Tali rischi sono identificati dall'IT Specialist.
- Risk Associated with Controls (RAwC): rischio associato al controllo. Tali rischi sono valutati dall'IT Specialist.

Il processo di valutazione del RAIT è composto da 3 elementi come mostrato in Figura:

1. Rischi derivanti dall'IT - La fase di valutazione dei rischi dell'ambiente IT (applicativi, database, sistemi operativi) prevede di assegnare sulla base di alcuni parametri, utilizzando il giudizio professionale, la System Risk Classification di tipo Higher o Not Higher. I fattori considerati sono quelli che impattano su:
    - **Financial Reporting** tra cui Pervasiveness to the business and financial reporting, Source Data, Data inputs and interfaces, Highly automated paperless processing, History of error in financial reporting related automatism
    - **Technology Platform** tra cui Type of application (custom o purchased), usage of systematic jobs, complexity of security.

Il RAIT può non coincidere con il RoMM valutato dall'audit sul saldo/asserzione del conto. Si può avere una situazione in cui si conclude che il RoMM è lower, ma il RAIT è higher.

Ad esempio, una società di distribuzione utilizza SAP per la gestione delle immobilizzazioni. SAP è classificato con RAIT Higher a causa del suo uso pervasivo, del numero di utenti, della complessità del modello di sicurezza, ecc. Inoltre, in SAP gli asset sono acquisiti e registrati in seguito a workflow automatizzati per l'approvazione, gli ammortamenti ed anche le plusvalenze o le minusvalenze da cessione sono calcolate sistematicamente. I RoMM associati a queste 3 classi materiali di transazioni sono classificati come Not Higher ma l'applicativo SAP rimane Higher.

2. Identificazione dei controlli per affrontare i rischi IT – Si identificano i General IT Controls (GITC) commisurati al rischio valutato derivante dall'IT, a seconda che sia lower, higher or significant, associato ad un sistema che tratta i dati contabili.
3. Testing Controls Based on Risk Associated with the Control - si testa il rischio associato al controllo (RAWC), ovvero il rischio che il controllo possa non essere efficace e, se non efficace, che ne risulti una deficiency significativa. La valutazione del rischio di material misstatements e del rischio associato al controllo determina la natura, i tempi e la portata dell'efficacia operativa del

controllo. Il rischio associato al controllo viene valutato come "higher" o "not higher" considerando i seguenti fattori:

- La natura e la rilevanza delle inesattezze che il controllo intende prevenire o rilevare;
- Se ci sono stati cambiamenti, rispetto all'anno precedente, nel volume o nella natura delle transazioni che potrebbero influenzare negativamente il disegno del controllo o l'efficacia operativa;
- Se il saldo del conto, la classe di transazioni o le informazioni fornite hanno una storia di errori;
- L'efficacia dei controlli a livello di entità, in particolare dei controlli che monitorano altri controlli;
- La natura del controllo e la frequenza con cui esso opera;
- Il grado con cui il controllo si basa sull'efficacia di altri controlli (ad esempio, l'ambiente di controllo o i controlli informatici generali);
- La competenza del personale che esegue il controllo o ne monitora le prestazioni e se ci sono stati cambiamenti nel personale chiave che esegue il controllo o ne monitora le prestazioni;
- Se il controllo si basa sulle prestazioni di un individuo o è automatizzato (ad esempio, un controllo automatizzato è generalmente considerato un rischio minore se i controlli informatici generali sono efficaci).

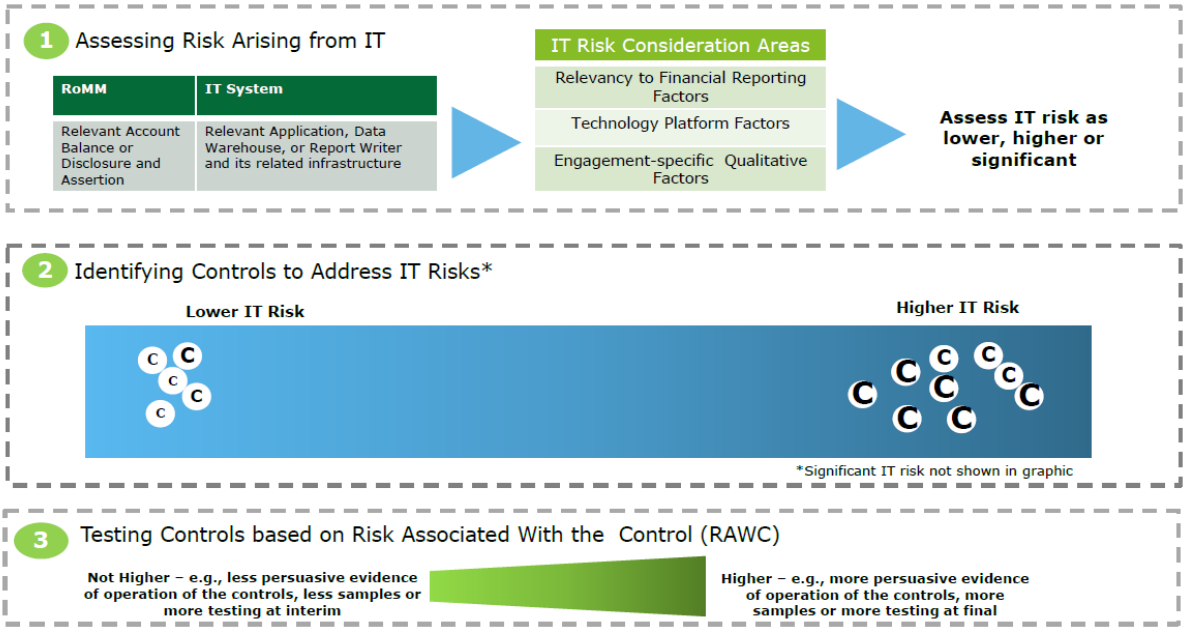


Figura 2.3

2.3.3 Documentare i controlli: GITC, ITAC, IPE

Come detto in precedenza, ogni entità effettua dei Controlli Applicativi al fine di presidiare i rischi relativi al processamento delle transazioni e dei dati di business all'interno di un Sistema Applicativo. La valutazione da parte del team di audit dell'attività di controllo effettuata dall'entità deve essere effettuata mediante **l'inquiry**, congiuntamente con una o più delle seguenti metodiche di verifica:

- Osservazione diretta dell'esecuzione del controllo;
- Analisi della documentazione e reportistiche varie;
- Reperformance del controllo.

Nel corso dell'**inquiry** si raccolgono **le seguenti informazioni**:

- Passi eseguiti nell'esecuzione del controllo
- Report ed altre informazioni utilizzate nell'esecuzione del controllo
- Procedure seguite in caso di eccezioni
- Procedure seguite in caso di assenza dell'owner
- Procedure seguite in caso di transazioni inusuali
- Modifiche ai controlli durante il periodo di audit, includendo cambi di personale che eseguono il controllo

L’obiettivo di taluni controlli, che possono essere di natura manuale e automatica, è garantire la:

- **Completezza:** l’elaborazione delle informazioni risultante dal processamento dei dati e delle transazioni risulta essere completa.
- **Accuratezza:** tutte le transazioni e i relativi dati vengono elaborati in modo accurato e le informazioni risultanti sono esatte;
- **Validità:** le transazioni e le elaborazioni dei dati generano informazioni valide
- **Riservatezza:** le informazioni sensibili sono protetti dalla divulgazione non autorizzata.

Sulla base degli applicativi identificati come rilevanti si effettua un’analisi sulla consistenza dei sistemi (GITC), dei test sui controlli automatici (ITAC) e verifica delle IPE e IUC rilevanti per l’intero processo di audit.

2.3.3.1 GITC

I General IT controls sono le politiche e le procedure che servono a supportare l'efficace funzionamento delle applicazioni, dei controlli automatici incorporati nelle applicazioni, l'integrità dei report generati da esse e la sicurezza dei dati ospitati all'interno delle stesse. I GITC si applicano alle seguenti aree:

1. **Access Security**, ovvero i controlli sugli accessi per prevenire o rilevare l’uso e le modifiche non autorizzati di dati, sistemi o programmi, verificando la presenza di una corretta segregation of duties.
2. **System Changes**, ovvero i controlli su Program Changes, acquisizione, modifica e manutenzione del software di sistema, acquisizione sviluppo e manutenzione del sistema applicativo.
3. **Data Center and Network Operations**, comprende i controlli per garantire l'integrità delle informazioni durante il loro trattamento, archiviazione o comunicazione da parte degli aspetti rilevanti dell'infrastruttura informatica

Nel caso di Access Security i rischi principali che potrebbero verificarsi sono un’impropria segregation of duties causata dal fatto che gli utenti hanno privilegi di accesso che vanno al di là di quelli necessari per l'espletamento dei compiti loro assegnati e l’apporto di modifiche inappropriate ai dati finanziari attraverso mezzi diversi dalle transazioni applicative.

Gli aspetti da considerare sono:

- Modalità di accesso (es. tecniche di autenticazione)
- Password policy
- Logging accessi ed eventi
- Parametri di Sistema
- Ciclo di vita di utenze e profili (creazione, modifica, cancellazione e review) con focus su:
    - Accessi degli utenti finali
    - Accessi dei super-utenti
    - Accessi diretti ai dati bypassando le normali procedure
    - Segregation of duties (SOD)

Nel caso di System Change Control i rischi principali che potrebbero verificarsi sono apporti di modifiche inappropriate a sistemi o programmi applicativi che contengono controlli automatizzati e/o logiche di report, modifiche inappropriate alla struttura del database e alle relazioni tra i dati ma anche al software di sistema (sistema operativo, network, change-management software, access-control software.

Gli aspetti da considerare sono:

- Metodologia e strumenti per la gestione dei change
- Ciclo di vita del sw/db (focus su collaudo e rilascio)
- Segregation of duties
- Modifiche in emergenza
- Separazione degli ambienti

Nel caso di Data Center and Network Operations i rischi che potrebbero verificarsi sono di accesso inappropriato alle informazioni di sistema se il network non impedisce in modo adeguato agli utenti non autorizzati di accedere. Si possono generare rischi di perdita di dati nel senso che non è possibile recuperare o accedere ai dati finanziari in modo tempestivo. Vi sono infine rischi legati alla sicurezza fisica se gli individui ottengono un accesso inappropriato alle apparecchiature del data center e sfruttano tale accesso per aggirare i controlli di accesso logici e ottenere un accesso inappropriato ai sistemi.

Gli aspetti da considerare sono:

- Accessi alla rete aziendale
- Accessi fisici e controlli ambientali
- Procedure di backup
- Modalità di gestione delle operation.

Tra gli aspetti rilevanti da sottoporre ad osservazione ci sono anche le interfacce tra i sistemi ed i datawarehouse, rappresentati in figura #.

I Datawarehouse contengono dati che confluiscono da sistemi diversi e che sono raccolti, normalizzati e gestiti in un unico “contenitore”, tipicamente per motivi di reporting. I dati confluiscono in tale “contenitore” tramite le interfacce.

Inoltre, quando sono presenti applicazioni che trasferiscono dati, aggregati o analitici, ad altre applicazioni, entrambi rilevanti ai fini dell’informativa finanziaria, è necessario considerare il rischio che i dati non siano trasferiti in maniera accurata e completa.

Tipicamente ci possono essere:

- interfacce automatiche, dove il trasferimento dei dati avviene in maniera automatizzata tra due applicazioni separate;
- Interfacce manuali, dove il trasferimento dei dati è eseguito manualmente dagli utenti.

Per entrambi gli ambiti è necessario individuare i principali controlli, manuali piuttosto che automatici da sottoporre ad analisi.

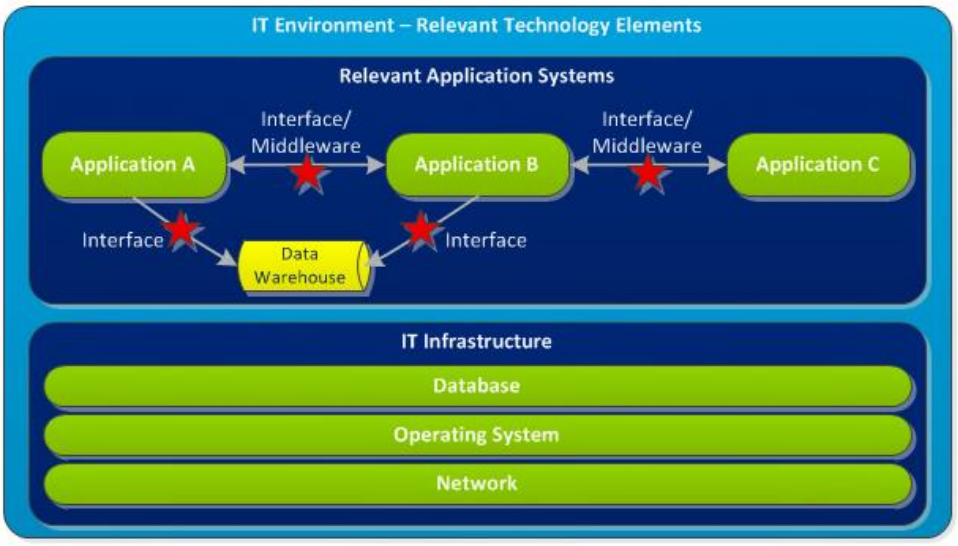


Figura 2.4

Le categorie di rischi presentate sopra si ripresentano in tutti i clienti, quindi, una volta identificati i rischi specifici applicabili alla singola azienda l'auditor va a valutare i controlli posti in essere da essa.

2.3.3.2 Controlli automatici (ITAC)

I controlli automatici sono incorporati nei sistemi applicativi e possono includere impostazioni configurabili, algoritmi automatici, calcoli automatici ed estrazione automatica dei dati. Data la natura della loro elaborazione di routine essi sono tipicamente più affidabili dei controlli manuali.

Sono testati per determinare se sono progettati, implementati e funzionanti in modo efficace.

Non è ovvio identificarli e documentarli perché spesso sono nascosti nella logica del sistema o dell'applicazione, tuttavia sono necessari per la possibilità di avere continuo monitoraggio attraverso dei tool.

A seconda del business possono variare, in quanto possono essere disposti tra le interfacce dei vari applicativi, possono regolare diverse logiche di SOD, possono regolare gli accessi e le soglie di accettazione per le fatturazioni. Le aree principali su cui si applicano sono:

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

Il test sul funzionamento dei controlli automatici si fa testando tutti i possibili scenari per ottenere evidenze sull'operatività degli stessi.

Ad esempio se il controllo automatico da testare è il blocco delle fatture nel caso in cui la differenza tra l'ordine d'acquisto e la fattura superi la soglia del 5%, si testano due scenari, una transazione inferiore al 5% (positive testing) con l'obiettivo di verificare che il controllo automatico ha elaborato la fattura come previsto e l'ha registrata in modo appropriato nell'A/P sub-ledger ed una transazione superiore al 5%(negative testing) per verificare che il sistema blocchi la transazione e la registri nel report delle fatture bloccate.

VALUTAZIONE CONTROLLI

In generale le dimensioni di valutazione del controllo sono sempre le stesse:

- Disegno ed implementazione
- Efficacia operativa.

Il disegno dei controlli è valutabile in termini di esistenza ed adeguatezza.

L'obiettivo di testare il design di un controllo è quello di determinare se esiste una deficiency nel disegno. Una deficiency nel disegno esiste quando:

- Manca un controllo necessario per soddisfare l'obiettivo di controllo (cioè un controllo che risolve il rischio di errori significativi).
- Un controllo esistente non è stato progettato correttamente.

L'esistenza del controllo viene valutata, tramite inquiry con il team IT della società auditata e/o ispezionando la documentazione richiesta a supporto delle analisi, verificando la presenza di:

- Disposizioni interne (regolamenti, procedure interne, manuali operativi, ecc.) che prevedono e disciplinano il controllo.
- Persone fisiche, ovvero i soggetti responsabili del controllo
- Procedure informatiche, che eventualmente supportano l'attività di controllo

L'adeguatezza del controllo si manifesta nel:

- Contenuto: idoneità tecnica del controllo a ridurre il rischio, nelle sue componenti impatto e probabilità
- Organizzazione: riferibile alle componenti risorse umane, stile informativo e di comunicazione, organizzazione del lavoro, risorse tecnologiche, ecc.
- Timing: preventivo (controllo capace di prevenire gli effetti provocati da un'anomalia) o consuntivo (controllo che consente di rilevare un errore/anomalia solo dopo che ha manifestato i suoi effetti)
- Ciclicità di effettuazione: frequenza con cui deve essere ripetuto il controllo (giornaliera, settimanale, mensile, annuale, ecc.)
- Livello di aggregazione
- Tracciabilità: documentabilità dell'attività di controllo

Si riporta in figura # un esempio di test del design sul controllo relativo allo user access per gli utenti dismessi.

Evaluation of Design Procedures		Evaluation of Design Testing Results
Inquire with management to understand the controls related to removing access to the application for terminated users. Specifically, consider obtaining an understanding of the following attributes, as appropriate: • Policies or procedures related to user provisioning; • How IT Management is notified of terminated users; • How access is removed or adjusted upon termination and if the same process is used for employees and non-employees (such as vendors, contractors, etc.); • Whether the process for removing access is manual or automated • Whether a tool is used to de-provision access • The method for removing access to the application (e.g., disabled or deleted); • Who has responsibility for security administration and changing user access when terminations occur; • What are the expectations for timely removal of user access (i.e., from date of separation to effective date of access modification).		Audit met with IT TEAM on 10/14/2019 to confirm how management proceed for removing access for terminated and/or transferred users in a timely manner (for Y Italia s.r.l. - PLACE Site, Y Friction Technologies - Ostrava (CZ) Site and WUXI China (PRC)). A summary of our procedures is highlighted below: Through corroborative inquiry performed with IT TEAM and supported by observation of documentation, we've been informed that user life cycle is managed as follows: User deletion We understood and reviewed that Y Italia s.r.l. (PLACE Site) has defined a workflow in Service Now for user deletion requests, "MT SAP Disable Account", working accordingly to the following process: - The Director of Human Resources communicates to the Payroll office all the information about the employee that quits job relationship with the company, then the payroll provides the information to all the heads of the other departments. - The deactivation form has to be signed by the requester and by the IT helpdesk for approval. - After deactivation approval, the IT TEAM proceeds for the deactivation (deletion within 30 days). The request is usually done by email. Based on the procedures performed above, we concluded that this control was designed effectively. No Exceptions Noted. Note: Audit performed procedures including inspection, observation, and/or reperformance in addition to corroborative inquiry to further confirm the implementation of this control. Our testing over the implementation of this control is tested in conjunction with our testing of operating effectiveness below, which details those procedures.
Evidence used to corroborate the design of the control		Process "Termination Notification Procedures"
Design Factor 1: Appropriateness of the Purpose of the Control and its Correlation to the Risk	Document considerations of the appropriateness of the purpose of the control and correlation to the IT risk identified.	The purpose of this control is to verify how Management manages access for terminated and/or transferred users is removed or modified in a timely manner. The removal of terminated users allows to not create improper access and segregation of duties. This control addresses the following IT risks: • Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.
Design Factor 2: Competence and Authority of the Person(s) Performing the Control	Control Owner(s) - Document considerations of the appropriateness of authority and competence of the process owner(s) to perform the control, including consideration of segregation of duties (as applicable)	Refer to the Summary worksheet for the evaluation of the competence and authority for individuals or groups performing the control.
Design Factor 3: Frequency and Consistency with Which the Control is Performed	Frequency of Control Operation	Audit noted the following in regards to the frequency of the control operation: • Considering the inherent risk related to this control, the control is appropriate. • The control is performed with "ad hoc" frequency: every terminated employee is removed.
Design Factor 4: Level of Aggregation and Predictability	Document considerations of the appropriateness of the levels of aggregation and/or predictability given the risk addressed	• The level of aggregation and predictability is normal as the control is manual in nature. • Management removals in a timely manner for terminated and/or transferred users are performed at an appropriate level of precision.
Design Factor 5: Criteria for Investigation and Process for Follow-up	Document considerations of the appropriateness of the criteria used for investigation (i.e., threshold) and the process for follow-up	Inspection of user list for a sample of resigned employees occurred during the Fiscal Year.
Evaluation of Design Conclusion		Effective

Figure 2.5 Design testing per il controllo Access for terminated and/or transferred users is removed or modified in a timely manner.

Una volta testato e concluso sull'efficacia del design, per ogni controllo, si segue una determinata procedura per valutare l'efficacia operativa.

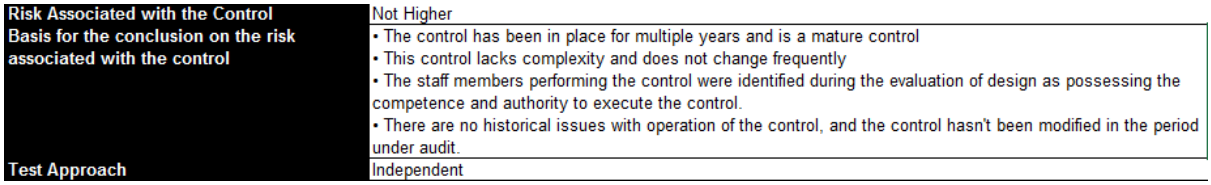
Quando si testa l'efficacia operativa di un controllo, si cerca di provare che esso funziona come dichiarato nel design. Se un controllo non è progettato correttamente, non può funzionare in modo efficace; pertanto, non è necessario determinare l'implementazione o verificare l'efficacia operativa di controlli progettati in modo improprio.

Testare l'efficacia operativa significa ottenere prove, positive o negative, per determinare se la procedura di controllo è stata eseguita correttamente (cioè, se tutti i passi importanti identificati nella descrizione dettagliata del controllo, di fatto, hanno funzionato come progettato o previsto, e per il periodo di reliance previsto).

L'obiettivo è di riuscire a riperformare il controllo effettuato dalla società eseguendo in modo indipendente le stesse procedure per confrontare se si ottengono gli stessi risultati.

- Come primo passo si definisce l'obiettivo del test, evidenziando in modo chiaro cosa costituisce una deficiency.
- Si definisce la popolazione da campionare.
- Si richiedono evidenze sufficienti ed appropriate, comprese le prove per verificare completezza e accuratezza delle IPE utilizzate per testare il controllo.

Nel determinare la pervasività dell'ispezione si tiene conto del rischio associato al controllo; si riporta in figura # un esempio di documentazione del rischio.



Risk Associated with the Control	Not Higher
Basis for the conclusion on the risk associated with the control	• The control has been in place for multiple years and is a mature control • This control lacks complexity and does not change frequently • The staff members performing the control were identified during the evaluation of design as possessing the competence and authority to execute the control. • There are no historical issues with operation of the control, and the control hasn't been modified in the period under audit.
Test Approach	Independent

Figura 2.6

La natura, il tempo e la portata delle prove dell'efficacia operativa, come detto in precedenza, dipendono dalla classificazione (Higher o Not Higher) del rischio assegnata nel RAWC come mostrato nella tabella successiva.

RAWC	Higher	Not Higher
Nature	Aumentare la pervasività del test, provando a riperformare il controllo effettuato dal cliente	Ispezionare attraverso inquiry, campionamento o osservazione le evidenze fornite
Timing (periodo da coprire con il test)	Eseguire i test a fine anno per ispezionare popolazioni più complete	Eseguire i test durante l'anno, non necessariamente alla chiusura del FY
Extent	Ispezionare campioni più grandi possibili	Ispezionare campioni di numerosità sufficiente

In particolare, indagare su se i controlli funzionano come progettati implica testare procedure e ottenere prove in merito a:

2. Evidenze di autorizzazione
3. Review di appropriate registrazioni

4. Processi di follow up sulle eccezioni.

Nella documentazione sull'efficacia operativa di un controllo devono essere presenti:

- Una descrizione delle prove ottenute
- Il periodo coperto dal test
- La dimensione del campione, compresa la frequenza del controllo
- Le procedure eseguite e le prove di efficacia operativa ottenute per ogni selezione.
- Una dichiarazione che non ci sono state eccezioni e che quindi il controllo è efficace o una chiara descrizione di eventuali deviazioni rilevate e la valutazione se la deviazione è una carenza.

Si riporta di seguito un esempio di test sull'efficacia operativa relativa allo stesso controllo 3 di cui si è già analizzato il design relativo all'accesso delle utenze terminate nel caso di Applicativo SAP.

Test Procedur	Operating Effectiveness Test Procedure (including Implementation)	Operating Effectiveness Test Results (including Implementation)
1	Obtain a listing of terminations for employees and contractors for the period of intended reliance from Human Resources. Make a selection of users that were terminated. For each user selected, test the following attributes: • Access privileges for the terminated user are no longer active in the system. Such access was removed, deleted or disabled in a timely manner (based on the effective date of the termination). ***Note 1: If a common key or field can be used to compare the termination listing to the listing of users, teams may consider performing a 100% test of all terminated users.*** ***Note 2: If teams are not performing a 100% test of all terminated users, teams may consider testing the timeliness of terminations for samples selected. Timeliness can be tested by generating SUIM change logs for the sampled users*** ***Note 3: Where tools (such as Tivoli Identity Management or others) are utilized to automatically remove access upon termination, teams may consider testing the termination control as an automated control. Additionally, if SAP authentication is integrated with the network operating system, this procedure may be covered as part of testing at the OS layer (Active Directory).*** ***Note 4: Listing of active users can be obtained through table USR02 or SUIM report or from ACTT raw output tables USR02, USR02CC, ADRP.***	In order to test this control we obtained a population of 281 resigned employees (on Audit date) for Y Italia s.r.l. - PLACE Site (63 resigned employees) and Y Friction Technologies - Ostrava (CZ) Site (98 resigned employees) and WUXI China (PRC) (120 resigned employees) from the " Y Termination List for Auditors 2019 - 12 - 06" provided by the GET - IT in the United States. In order to perform the 100% test of all terminated users, we crossed the list provided with the list of active users in SAP coming from table USR02 for FY18 and FY19 in order to check: - how many terminated employees in FY19 had access to SAP in FY18 (48); - how many among the employees that were hired in FY19 but also were terminated in FY19 had access to SAP during FY19 (5). We observed that 3 users seemed to have logged on after their termination date; - Jianqiao Shentu, Termination Date: 8/9/2019; LLO: 8/12/2019 - Aria Ye, Termination Date: 11/8/2019; LLO 11/13/2019 - Walter Beltrando, Termination Date: 3/16/2019; LLO 10/1/2019 So, after our analysis three exceptions were identified: BGBW: Being this a user of radio frequency, IT TEAM did not received any email from either the production department or the warehouse department, as usual for a user of radio frequency like this one; hence this user was not immediately associated with Beltrando Walter. Successively, IT TEAM said that the user BGBW was mistakenly created and this was not a user of radio frequency. The root cause of this exception was an error in the naming convention. The last log on was on the 29/05/2019. We understood that the user account was shared within the manufactory plant department for service activities (SM20 log of BGBW activities was reviewed by IT dept.) and the user account has now been removed from SAP. JSHENTU and AYE: These users were interns for WUXI China,; according to IT TEAM CHINA, the comunication of the termination of these people was inserted into the application Workday after the actual termination of the intern with the business department being aware of the situation; Denny who was the person in charge for blocking the user in a timely manner , received the information orally the first working day following the termination of Jianquiao Shentu and Aria YE (the employees were infact separated on a Friday, Denny received the information the following Monday) but not in time to prevent the user access. Through corroborative inquiry with IT TEAM, we received the SM20 log for the users JSHENTU and AYE for the days between the termination day of the employee and the last logon date. The log was reviewed by IT TEAM MANAGER and the user account has now been removed from SAP. Among the 53 employees who had access in SAP in between the current fiscal year and the past fiscal year we selected a sample of 5 terminated users based on Methodology. The analysis is embedded below within the Excel file attached The results are presented in sheet SAP.02a.
Mitigating Procedures		Factors Indicating Why Identified Mitigating Controls Address the IT Risk: 1.The company performs a lookback analysis regarding the activities done by the users 2. The Company can identify users inactive from more than 90 days and delete them thanks to a monthly review. Mitigating Controls: 1. Management perform a review of inactive users from more than 90 days in order to identify and delete these users. The next one will be performed at the end of Q4 so it will be available in January 2019. However, the users sampled have already been disabled by IT TEAM in early November. 2. SAP.03: End User access is periodically reviewed. 3. Management confirmed us that the identified users didn't exploit access following their resignation CONCLUSION: Audit noted that this control is operating effectively.

Figure 2.7 Operating Effectiveness testing per il controllo Access for terminated and/or transferred users is removed or modified in a timely manner.

Una volta completato il testing, secondo la modalità prescelta, si avrà un quadro dei rischi e dei controlli con la relativa valutazione.

Risk Arising from IT (RAIT)	RAIT Risk Classification	If RAIT Risk Classification differs from System Level IT Risk Classification, document Rationale	Control ID	Control Description	Risk Associated with Control	Test Approach	Design Conclusion	Final Operating Effectiveness Conclusion	Risk Conclusion	Deficiencies Noted?
Production systems, programs, and/or jobs result in inaccurate, incomplete or unauthorized processing of data.	Higher	No	SAP.15	Only authorized users have access to update the batch jobs (including interface jobs) in SAP.	Not Higher	Independent	Effective	Effective	Addressed	No
			SAP.16	Critical jobs are monitored, and processing errors are corrected to ensure successful completion.	Not Higher	Independent	Effective	Effective		No
Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	Higher	No	SAP.01	Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles, critical financial reporting transactions, and segregation of duties.	Not Higher	Independent	Effective	Effective		No
			SAP.02	Access for terminated and/or transferred users is removed or modified in a timely manner.	Higher	Independent	Effective	Effective		Yes
			SAP.03	User access is periodically reviewed.	Not Higher	Independent	Effective	Effective		No
			SAP.04	Segregation of duties is monitored and conflicting access is either removed or mapped to mitigating controls, which are documented and tested.	Higher	Independent	Effective	Effective		No
			SAP.06	Access to security administrative functions is authorized and appropriately restricted.	Not Higher	Independent	Effective	Effective		No
			SAP.07	Table update access is restricted based on specific business need. Users with table edit transaction access are restricted to defined tables based on job responsibilities.	Not Higher	Independent	Effective	Effective		No
			SAP.11	Access to change the password parameters is granted appropriately based on job responsibilities.	Not Higher	Independent	Effective	Effective		No
			SAP.17	Users are authorized to execute programs based on their job responsibilities and restricted to specific programs required. Access to all transaction codes is not granted to users.	Not Higher	Independent	Effective	Effective	Addressed	No
			SAP.18	Powerful profiles SAP_ALL and SAP_NEW are adequately secured by ensuring no dialog or service user has access to these profiles.	Higher	Independent	Effective	Effective		No
			SAP.19	Remote access to SAP for software maintenance for the SAP vendor is restricted, approved by management, and removed in a timely manner. Access to the SAP Support IDs is appropriately controlled when IDs are not in use.	Not Higher	Independent	Effective	Effective		No
			SAP.20	Emergency access to SAP is permitted only with prior approval, logged, monitored by someone other than users who administer the access and removed in a timely manner.	Not Higher	Independent	Effective	Effective		No
Systems are not adequately configured or updated to restrict system access to properly authorized and appropriate users.	Higher	No	SAP.05	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorized to gain access to the system. Password parameters meet company and/or industry standards (e.g., password minimum length and complexity, expiration, account lockout).	Not Higher	Independent	Effective	Effective	Addressed	No
			SAP.09	The default passwords for standard SAP IDs have been changed in all clients and secured appropriately. If access to one of these powerful user accounts is required, the request is documented, approved by management, and access is removed upon completion of the request.	Not Higher	Independent	Effective	Effective		No

Figure 2.8 Control and Testing Summary

2.3.3.3 IPE e IUC

Quando l'auditor utilizza le informazioni prodotte dall'entità come elementi probatori della revisione (come evidenze), l'auditor deve effettuare un ulteriore controllo sulle informazioni, al fine di valutare se sono sufficienti, appropriate e dettagliate.

Si testano dunque due tipi di dati, le IUC e le IPE.

Un'IPE è un Information Produced by the Entity, ovvero qualsiasi report, fornito dalla società auditata, contenente informazioni estratte da sistema e/o inserite manualmente, utilizzato per eseguire un'attività di controllo rilevante. Vedi figura #.

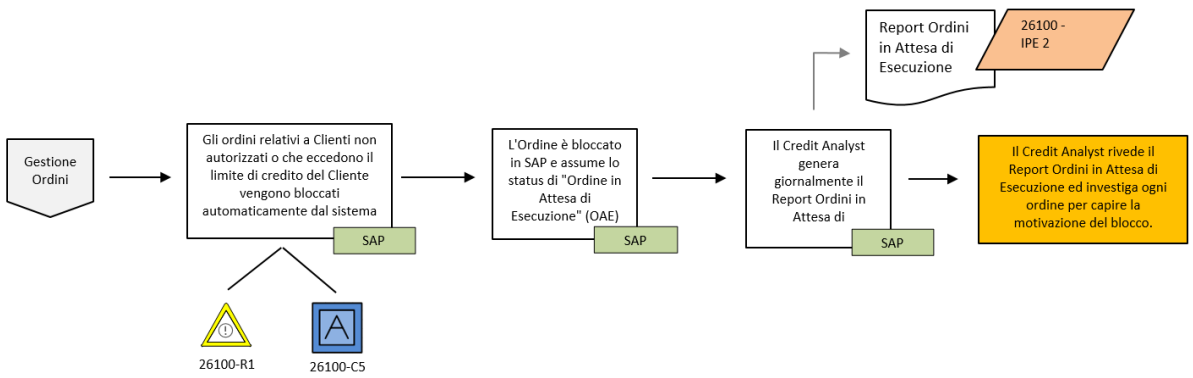


Figure 2.9 Esempio di IPE

Le IUC o *Information used in a control* sono delle IPE utilizzate dal cliente per eseguire i propri controlli rilevanti.

Le IPE in generale sono testate a fronte di verificare problematiche quali:

- Parametri inseriti a sistema per l'estrazione dei report non corretti
- Dati estratti non completi
- Logica applicativa errata
- Modifiche non autorizzate ai dati sorgente o alla logica applicativa.

Una IUC è composta da tre elementi, source data, report logic, parameters.

- Source Data: è la fonte da cui nasce la IUC. Essa può includere dati conservati nel sistema informatico (ad esempio, all'interno di un sistema applicativo o di una banca dati) o esterni al sistema (ad esempio, dati conservati in un foglio di calcolo Excel o conservati manualmente.
- Report Logic (la logica del report automatizzato) sono le query, gli algoritmi o le formule per trasformare, estrarre o caricare i dati di origine rilevanti e creare il report. La report logic può includere programmi di generazione di report standardizzati, strumenti gestiti dall'utente (ad esempio, strumenti di interrogazione e redattori di report) o fogli di calcolo Excel.
- Report Parameters: sono i parametri inseriti per la generazione di report contenenti le sole informazioni di interesse. I parametri del report possono essere inseriti manualmente dall'utente o possono essere preimpostati e possono essere o meno soggetti ai controlli generali dell'IT. Vedi figura #.

L'IT auditor procede a verificare che i parametri inseriti a sistema siano presenti sul report e che essi siano coerenti con quelli impostati a sistema dall'owner del controllo e ne riporta opportune evidenze.

Per quanto riguarda la Report Logic tipicamente la metodologia di testing consiste nel riperformare la logica che ha portato alla generazione del report. Esempi di test sono:

- Analisi delle query utilizzate per l'estrazione e generazione del report.
- Riperforming delle logiche di calcolo del report (manualmente o con tool automatici), assicurandosi di considerare tutte la variabili significative.

Per testare accuratezza e completezza sono effettuati rispettivamente:

- Selezione di un campione di dati dalla sorgente e riconciliazione con le informazioni presenti nel report
- Riconciliazione di tutti i record del report con la totalità delle informazioni della sorgente dati.

Poiché la IUC viene generata in molte forme diverse e attraverso metodi diversi, la strategia di valutazione del team di audit può variare a seconda della natura della IUC (ad esempio, un rapporto standard precodificato rispetto a un rapporto ad hoc personalizzato). Di seguito, in figura # si riporta un esempio di IUC relativa all'applicativo RDS.

Control Summary	
Application/Technology	**RDS - Accounting System**
Control Name	*Manual Journal Entries are reviewed by a different person than the one who prepared the entry.*
Control ID	**ITRFSC2**
Control Activity Description	Every month, through a query of RDS, the Chief Accountant XX extracts the general ledger for the month interested by the control: the query contains two parameters, the Company and the period. The report extracted is an Excel file that lists every line of the entries posted in the period, the relative amounts and the user who posted them.
Ref. Working Paper Audit Control	**see w.p. 15238.1**

IUC Background	
IUC Background	The IUC is the *Monthly General Ledge*r that is reviewed by a different person that the one who prepared the entry. The IUC was generated from instance of RDS.
Manual or System Generated?	System Generated
Date Generated	**January:** 12.02.2019 **February:** 13.03.2019 **March:** 09.04.2019 **April:** 10.05.2019 **May:** 03.06.2019
Source System	RDS - Accounting System
Procedure(s) Performed over Report Logic	Auditor noted that Management's control over the logic of the report relies on the automated nature of the logic and reliance on the change management controls to confirm that the logic is not altered inappropriately. Auditor observed on 12.02.2019, 13.03.2019, 09.04.2019, 10.05.2019, 03.06.2019 and xxxxxxx,the logic used by management behind the report that generates the Cedolone Monthly The logic observed within the report corresponded with the purpose of the system generated report. Additionally, Auditor tested the application access and change management controls within w.p. 20105.01 (these controls were designed and operating effectively throughout the period subject to our audit): Auditor observed and noted the automated nature of the generation of the report based on the stored logic covered by change management. Auditor also inquired with control owners at multiple times during the audit period to ascertain that: 1. The listing is created from the relevant source; 2. No Modifications/filters were made to the report generated; 3. The relevant fields/attributes, corroborated via design inquiry and inspection of the program logic, were present in the report; 4. The users and supporting security details in the system were consistent with those reflected in the report based on our discussion and inquiries with control owners. Auditor obtained the query's code [IA Dati per Revisori – APAMPNCT [CUSTOM]] use to Journal Entry's extraction. It 's a RDS custom query. Auditor analyzed the query structure and there aren't parameters that would limit the population when extracting the report. Query [IA Dati per Revisori - APAMPNCT [CUSTOM]]: Document
Procedure(s) Performed over Report Parameters	Auditor noted that management relies on the manual input of parameters: 1. Company Code [Sigla] 2. Date [Data registrazione] See Screenshot#1. Details of each monthly extraction. Auditor noted that management's controls over parameters were found to be effective.
Procedure(s) Performed over Report Source Data	Source Data: all journal entries Auditor performed testing of controls over the accuracy and completeness of the IUC. Auditor noted that the source data of the report output sits in security tables within RDS Database. Auditor noted that XX, Chief Accountant YY, set report parameters for the generation of the report/IUC as noted above. Additionally, Management relies on the automated access restriction and change management controls. Management evaluates source data as part of the following access and change management controls (these controls were designed and implemented/operating effectively). Please see w.p. 15238.1 sheet "ITRBFS2" and sheet "Implementation" to analyze the Source Data controls implemented to Audit Team. Auditor noted that management's controls over report source data were found to be effective.
Conclusion	**Complete and accurate**

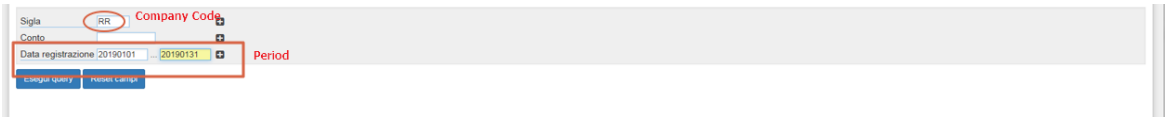
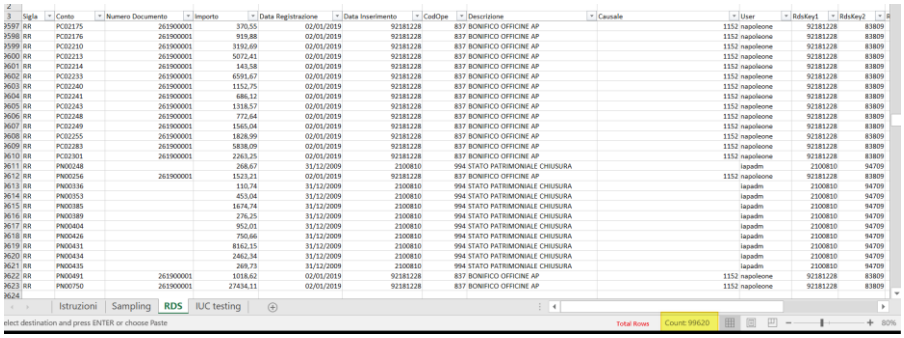


Figure 2.10 Parametri inseriti a sistema



Sigla	Conto	Numero Documento	Importo	Data Registrazione	Data Inserimento	CodOpe	Descrizione	Causale	User	RdsKey1	RdsKey2
RR	PC02175	261900001	370,55	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02176	261900001	919,88	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02210	261900001	3192,69	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02213	261900001	5072,41	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02214	261900001	143,58	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02233	261900001	6591,67	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02240	261900001	1152,75	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02241	261900001	686,12	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02243	261900001	1318,57	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02248	261900001	772,64	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02249	261900001	1565,04	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02255	261900001	1828,99	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02283	261900001	5838,09	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PC02301	261900001	2263,25	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PN00248		268,67	31/12/2009	2100810	994	STATO PATRIMONIALE CHIUSURA		iapadm	2100810	94709
RR	PN00256	261900001	1523,21	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PN00336		110,74	31/12/2009	2100810	994	STATO PATRIMONIALE CHIUSURA		iapadm	2100810	94709
RR	PN00353		453,04	31/12/2009	2100810	994	STATO PATRIMONIALE CHIUSURA		iapadm	2100810	94709
RR	PN00385		1674,74	31/12/2009	2100810	994	STATO PATRIMONIALE CHIUSURA		iapadm	2100810	94709
RR	PN00389		276,25	31/12/2009	2100810	994	STATO PATRIMONIALE CHIUSURA		iapadm	2100810	94709
RR	PN00404		952,01	31/12/2009	2100810	994	STATO PATRIMONIALE CHIUSURA		iapadm	2100810	94709
RR	PN00426		750,66	31/12/2009	2100810	994	STATO PATRIMONIALE CHIUSURA		iapadm	2100810	94709
RR	PN00431		8162,15	31/12/2009	2100810	994	STATO PATRIMONIALE CHIUSURA		iapadm	2100810	94709
RR	PN00434		2462,34	31/12/2009	2100810	994	STATO PATRIMONIALE CHIUSURA		iapadm	2100810	94709
RR	PN00435		269,73	31/12/2009	2100810	994	STATO PATRIMONIALE CHIUSURA		iapadm	2100810	94709
RR	PN00491	261900001	1018,62	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809
RR	PN00750	261900001	27434,11	02/01/2019	92181228	837	BONIFICO OFFICINE AP	1152	napoleone	92181228	83809

Istruzioni | Sampling | RDS | IUC testing

Figure 2.11 Valutazione accuratezza del report

Le IPE sono valutate in modo simile alle IUC. I test effettuati sono diversi a seconda di *custom report* o *standard report*. Gli *standard report* sono quelli prodotti da un applicativo di cui il cliente non dispone del linguaggio sorgente e quindi non ha la possibilità pratica di effettuare modifiche alla logica. Per i c*ustom reports invece* l'accuratezza dell'algoritmo di estrazione è da testare, in quanto le query sono disponibili.

Per i *custom report* allora l'indagine dell'IT auditor è su:

- Source Data
- Report Logic: Algoritmo di estrazione (Query script) e algoritmo di generazione di informazioni automatiche contenute nell'IPE
- Parametri di input

Per gli *standard report invece l'*indagine dell'IT auditor è solo su:

- Source Data
- Parametri di input

In figura #, si riportano tre esempi di IPE su SAP.

Name of Report	Source of Report	Standard/ Custom?	Report Owner	Date Generated	How did the report come into scope? (i.e. Planning, Performing Tests of Operating Effectiveness of Controls, Substantive Analytical Procedures, Tests of Details)	Purpose of Report (i.e. To support a review of A/R Aging)	Source Data	Report Logic	Manual Parameters	Management Control over IPE	Conclusion Regarding the Integrity, Completeness and Accuracy of the Key Report ("Effective" or "Not Effective"
Report HFM - Headcount (GD13)	SAP ECC8 - PRD	Standard (please see sheet 'Appendix' for further details over mapping reports to the associated program)	XX (SAP Specialist)	List of Totals Record Display.	Planning	The Report "HFM" used for Audit Test (Italy, Czech republic and China) is produced by HFM system managed by Company Y Headquarter and contains the same values inserted into SAP.	Through corroborative enquire with XX (SAP Analyst) we detect that the data source are generated from SAP through the GD13 transaction (Totals Record Display - FI Basic Functions) used to produce data useful for Central HFM report. This is a standard transaction from SAP ECC8 system.	Through corroborative enquire with XX (SAP Analyst) we verify that report is standard as part of the package software and it has not been modified by Company. For this reason no further testing procedures on the report logic have been performed.	Through corroborative enquire with XX (SAP Analyst) we have inspected the parameters (for Italy, Czech Republic and China companies) used to execute the transaction GD13 to inspect the completeness of the data selected for the report: - Company Code: Z001 (Italy) / Z040 (Czech Republic) / Z042 (China); - Extraction Period: from 01-01-2019 to 18-11-2019.	N/A	Effective
KE24	SAP ECC8 - PRD	Standard (please see sheet 'Appendix' for further details over mapping reports to the associated program)	XX (SAP Specialist)	List of all Delivery Notes for the incoterms analysis.	Planning	The Report is used for Audit Test (Italy, Czech republic and China) about the Delivery Notes for the incoterms analysis .	Through corroborative enquire with XX (SAP Analyst), we detect that the data report are generated from SAP through the KE24 transaction (Line Item Display_Actual Data - Profitability Analysis). This is a standard sap transaction from SAP ECC8 system.	Through corroborative enquire with XX (SAP Analyst) we verify that report is standard as part of the package software and it has not been modified by Company. For this reason no further testing procuders on the report logic have been performed.	Through corroborative enquire with XX (SAP Analyst) we have inspected the parameters (for Italy, Czech Republic and China companies) used to execute the transaction KE24 to inspect the completeness of the data selected for the report: - Company Code: Z001	N/A	Effective
FBL5N	SAP ECC8 - PRD	Standard (please see sheet 'Appendix' for further details over mapping reports to the associated program)	XX (SAP Specialist)	List of Custumer Ledgers.	Planning	The Report is used for Audit test (Italy, Czech republic and China) about the Custumer Ledgers.	Through corroborative enquire with XX (SAP Analyst), we detect that the data report are generated from SAP through the FBL5N transaction (Customer Line Items - FI Information System). This is a standard SAP transaction from SAP ECC8 system.	Through corroborative enquire with XX (SAP Analyst) we verify that report is standard as part of the package software and it has not been modified by Company. For this reason no further testing procuders on the report logic have been performed.	Through corroborative enquire with XX (SAP Analyst) we have inspected the parameters (for Italy, Czech Republic and China companies) used to execute the transaction FBL5N to inspect the completeness of the data selected for the report:	N/A	Effective

Figure 2.12 Esempio di IPE

Sia le IPE che le IUC si concludono con l'attribuzione dell'efficacia del report o della deficiency.

2.3.4 Valutazione delle deficiency

Le deficiency relative a un controllo possono essere di 3 tipi, secondo la classificazione del PCAOB si ha:

1. **Material weakness** se esiste una ragionevole possibilità che un'inesattezza sostanziale del bilancio d'esercizio o del bilancio intermedio della società non venga impedita o rilevata in modo tempestivo
2. **Significant deficiency** se è meno grave di una material weakness, ma abbastanza importante da meritare l'attenzione dei responsabili della supervisione della rendicontazione finanziaria della società
3. **Deficiency** se il design o il funzionamento di un controllo non consente al management o ai dipendenti, nel corso del normale svolgimento delle funzioni assegnate, di prevenire o rilevare tempestivamente eventuali inesattezze.

In presenza di controlli il cui testing ha dato esito negativo (controlli inefficaci da un punto di vista di D&I e/o OE), è necessario effettuare ulteriori riflessioni in maniera tale da valutare l'effetto di tali carenze (deviazioni o deficiency) sugli IT risk.

Per ognuno di questi controlli si indaga sulle seguenti:

- Ci sono altri controlli generali IT che sono "a copertura" dell'IT risk sottostante?
- Ci sono dei controlli di business diretti che sono "a copertura" dell'IT risk sottostante?

Nel caso in cui non ci fossero, è necessario procedere a valutare ulteriormente gli IT risk non coperti rivalutando ed integrando:

- Le procedure substantive;
- Le valutazioni degli application controls e degli IPE che sono gestiti nell'IT environment nel quale sono presenti queste carenze.

Altrimenti, è sufficiente documentare e collegare appropriatamente le procedure alternative, gli altri controlli generali IT compensativi (ottenendo prove sufficienti della loro efficacia) o gli altri controlli diretti al controllo nel quale è presente la deficiency.

Tra gli esempi di questioni che il revisore può prendere in considerazione nel determinare se una deficiency o una combinazione di deficiency nel controllo interno costituisce una deficiency significativa vi sono:

- La probabilità che le deficiency portino in futuro a significative inesattezze nel bilancio.
- La suscettibilità alla perdita o alla frode della relativa attività o passività.
- Variazioni sugli importi di bilancio.
- Il volume di attività esposte alla deficiency.
- La causa e la frequenza delle eccezioni rilevate a seguito delle deficiency dei controlli.
- L'interazione della deficency con altre deficiency nei controlli interni.

Le procedure di mitigazione aiutano a determinare se l'esposizione potenziale causata dalla deficiency è mitigata o se è necessario notificare alla società la carenza del controllo.

Esempi di deficiency e procedure di mitigazione sono riportati di seguito:

EVIDENZE DA RICHIEDERE	DEFICIENCY E PROCEDURE MITIGATIVE
System log with last user logon date	Si è scoperto che 15 dipendenti dismessi avevano accesso alla revenue application della società. Si indaga sui dettagli degli ultimi login degli stessi successivi alla data di dismissione. Se gli utenti non hanno effettuato l'accesso all'applicazione la deficiency è mitigata.
System log with production changes	Due individui IT hanno accesso a sviluppare cambiamenti e migrarli verso la produzione (mancanza di SOD). Si indaga sui record delle modifiche all'interno del sistema. Se nessuna modifica di programma o di configurazione è stata migrata in produzione da questi due utenti la deficiency è mitigata.

Un esempio di evaluation of deficiency sul controllo 2 relativo agli accessi di utenti dismessi sull'applicativo SAP è riportato di seguito.

Deficiency Status at Year-end (Open/ Unremediated, Closed/ Remediated)	Relevant General IT-Technology Layer(s)	Control Reference	Area of IT Controls	Risk Arising from IT ("IT Risk")	Determine the Nature and Cause of the Deficiency (Refer to Note 2 for items to consider, such as the nature and cause of the deficiency and the scenario or "what could go wrong" as a result of the deficiency)	Are there mitigating procedures that address the IT risk? If so, describe below	Are there other general IT controls that address the IT risk? If so, describe below	Are there direct controls that address the IT risk? If so, describe below	Is the IT risk addressed by controls ?	If IT risk not addressed by controls , is the IT risk mitigated by AUDIT mitigating procedures?	Consider the effect of the deficiency and the need to modify the audit plan?	Conclusion (D, SD, MW)	Basis for Conclusion About Severity	Conclusion (N/C, SD, MW)	Basis for Conclusion About Severity
Closed/Remediated	Application - SAP PRD	SAP.02	Access Security	Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	Italy: in mid october there was a user ID of a resigned employee (BGBW Walter Beltrando) that was not deleted in timely manner. After inquiry with IT TEAM, AUDIT noted that the user ID BGBW was a user of radio frequency classification type, hence this user was not immediately associated with Beltrando Walter for the termination process. Successively, after inquiry, IT TEAM said that the user BGBW was mistakenly created as radiofrequency type at the beginning. The root cause of this exception was an error in the naming convention. China: two user accounts (Jiangjiao Shentu - JSHENTU, Aria Ye - AYE) retained access to SAP after the users were terminated from the company and logged into SAP PRD3 after those employees were terminated, both of them are interns present in the company for the less than 3 months. The root cause of the China issue was related to the business needs of the Intern Managers communicate orally to the IT Department and a late communication of users termination from HR dept. through Workday application.	N/A - There were no mitigating procedures performed by AUDIT, as effective mitigating controls were identified.	Mitigating Controls: SAP.03: User access is periodically reviewed. CONCLUSION: AUDIT noted that this control is operating effectively. Please refer to the local engagement team audit file for a summary of testing procedures performed. Factors Indicating Why Identified Mitigating Controls Address the IT Risk: 1. Management perform a look back analysis review of user, in particular through SM20 log analysis for BGBW. JSHENTU and AYE in order to identify and delete these users.Management confirmed us that the identified users didn't exploit access following their resignation using business as usual transactions. 2. Should a non-active employee or contractor appear in the listing, it would be detected by management and flagged for IT Administrators of the respective technology to remove access that is no longer required. 3. AUDIT further observed that users were not captured during the user access review process as they were terminated after the completion of the review, thus this did not provide contradictory evidence regarding the effectiveness of the user access review. The users have already been disable by IT TEAM and Danny Zhao. Based on the factors outlined above, we feel that the below mitigating controls address the IT risk.	N/A - Risk addressed by GITCs	Yes	N/A - Risk is addressed by GITCs	No - There is no need to modify the audit plan, as the IT risk is addressed through mitigating controls.	D	AUDIT noted that this control is not operating effectively. AUDIT noted that two users have not been deleted or locked after the users's assignees resigned. AUDIT noted that some users assigned to resigned people from China and Czech Republic logged into the SAP	N/C	Following the guidance within decision tree B, from Chapter 6 of the internal control guide, we noted that alternative mitigating controls were designed & performed by management that address the associated risk. As a result, we considered the guidance

Figure 2.13 Evaluation of deficiency on control Access for terminated and/or transferred users is removed or modified in a timely manner.

2.3.5 Analisi aggiuntive - JET

Il JET (Journal Entry Test) è un test effettuato sul libro giornale della società auditata. Per redarre il JET il team di audit ha bisogno del Libro Giornale della società e del Bilancio di Verifica per indagare sulla presenza di eventuali squadrature tra essi.

Una volta effettuata la quadratura si procede con 11 test selezionati per evidenziare scritture anomale all'interno del libro giornale. Essi sono:

- **Test01 – Registrazioni su conti inusuali:** identifica le registrazioni effettuate su conti inusuali. La selezione dei conti avviene manualmente in base alla descrizione (e.g. «non usare») oppure in base al piano dei conti, su giudizio dell'audit
- **Test02 – Registrazioni su conti poco usati:** identifica le registrazioni effettuate su conti con meno di X registrazioni nel periodo in esame.

- **Test03 – Registrazioni su conti non correlati**: identifica le registrazioni effettuate su conti non correlati, in base alle associazioni create nel file «General Parameters.xls» (es.: registrazioni di vendite in avere con contropartita nei debiti verso clienti).
- **Test04 – Debiti a Ricavi**: identifica tutte le registrazioni il cui risultato complessivo è un debito nei ricavi e maggiori dell'importo impostato.Il test serve ad identificare eventuali storni di ricavi registrati nel trimestre precedente.
- **Test05 – Utenti con poche registrazioni o utenti di interesse**: identifica tutte le registrazioni effettuate da utenti con meno di X registrazioni nel periodo in esame. Il test conteggia diversamente le registrazioni standard da quelle non-standard, quindi ad esempio un utente che effettua solo registrazioni standard, viene identificato dal test se effettua anche meno di X registrazioni non-standard.
- **Test06 – Registrazioni di chiusura:** identifica tutte le registrazioni effettuate nel periodo di chiusura del trimestre con data di competenza nel trimestre in oggetto e il cui effetto complessivo è un aumento/riduzione di Attivo/Passivo/Ricavi/Costi maggiore della soglia impostata.
- **Test07 – Registrazioni inserite dopo la chiusura del trimestre:** identifica tutte le registrazioni effettuate dopo la data di chiusura del trimestre, con competenza nel trimestre in oggetto.
- **Test08 – Registrazioni in date di interesse:** questo test identifica le registrazioni effettuate nel weekend, nelle festività, o in giorni infrasettimanali di interesse.
- **Test09 – Registrazioni con parole chiave di interesse nella descrizione:** questo test identifica le registrazioni che contengono le parole chiave all'interno della descrizione.
- **Test10 – Registrazioni con importi tondi o cifre ricorrenti:** questo test identifica le registrazioni che contengono importi tondi (es.: 100.000€) oppure con un numero di cifre ricorrenti (es.: 29.999 €).

- **Test11 – Registrazioni con duplicati:** questo test identifica le registrazioni che contengono importi duplicati (es.: che contengono la stessa combinazione di righe/conti e importi) e che sono ripetute più di X volte.

2.4 Verso una nuova direzione

Fino a poco tempo fa, la professione dell'Internal Audit non ha affrontato la necessità di innovare e tanto meno di reinventarsi. Si può far risalire la nascita del moderno Internal Audit - "Internal Audit 1.0" - alla fondazione dell'Institute of Internal Auditors (IIA) nel 1941 - e far risalire "Internal Audit 2.0" alla Sarbanes Oxley e al suo impatto sulla professione contabile. Lungo il percorso, sviluppi come il framework COSO, il miglioramento di capacità dell'audit interno e l'analisi dei dati, hanno contribuito a far progredire la professione. Ora, però mentre ci si avvicina alla fine di un decennio di inquietante incertezza, le organizzazioni devono affrontare una nuova evoluzione strategica, operativa e nuovi rischi operativi ed informatici. Il mondo sta entrando nella quarta rivoluzione industriale dove le nuove tecnologie, la digitalizzazione e l'intelligenza artificiale stanno cambiando radicalmente il panorama del business e le figure al suo interno. Per tale ragione, le società di consulenza stanno adesso considerando nuovi modelli di business che prevedono l'integrazione di nuove piattaforme digitali che permetteranno all'audit di adottare nuovi approcci per testare i rischi e i controlli, che possono essere in parte abilitati dalle nuove tecnologie digitali dirompenti:L'RPA.

CAPITOLO 3

Le organizzazioni hanno sempre cercato modi per ottenere una maggiore efficienza operativa e sostenere la crescita attraverso l'automazione dei processi. Nel corso dei decenni le attività puramente manuali sono state via via automatizzate con l'avanzare del progresso tecnologico.

Per le operazioni interne di un'azienda moderna, il principale abilitatore dell'automazione è stata la tradizionale tecnologia dell'informazione (IT). Molte organizzazioni hanno applicato la tecnologia ai processi aziendali attraverso l'uso di ERP e altre applicazioni aziendali. Tuttavia, alcune di queste stesse organizzazioni hanno ancora un mosaico di processi e applicazioni aziendali non ottimali che non si parlano tra loro e che raramente alleviano il carico di lavoro per generare intuizioni

significative. Ciò che si traduce in un aumento dei costi, tempi di ciclo inutilmente elevati, qualità non uniforme e agilità compromessa.

Una possibile spiegazione di questa situazione è la crescita: poche aziende gestiscono la crescita del business in modo sistematico.

Finora le organizzazioni hanno risposto a questa sfida in vari modi, tra cui:

1. Investendo in applicazioni aziendali migliori o meglio integrate. Teoricamente, questo rappresenta tipicamente l'approccio "giusto", ma tali progetti sono costosi e molte implementazioni falliscono. Anche i progetti che dimostrano di avere successo possono richiedere anni per essere implementati, e qualsiasi sforzo per ridurre i tempi di realizzazione può compromettere le possibilità di successo e aumentare il rischio di fallimento. I costi di gestione possono essere ancora elevati dopo il completamento, e i lunghi tempi di implementazione possono limitare l'agilità.
2. Ottimizzando i processi con l'aiuto di una BPMS - un'applicazione software che supporta il ciclo di vita del miglioramento del processo, e spesso facilita l'integrazione tra le applicazioni aziendali per aumentare la quantità di "straight-through processing" possibile all'interno di un processo. In effetti, si tratta di un approccio simile a quello di una trasformazione IT, ma con una portata più ridotta rispetto all'ERP. Sono generalmente meno costosi e meno rischiosi da realizzare, ma possono anche offrire vantaggi ridotti.
3. Sviluppando servizi condivisi e/o esternalizzando i processi a un fornitore terzo di Business Process Outsourcing (BPO), che tipicamente otterrà efficienza attraverso l'arbitraggio del lavoro e in virtù della scala. Si tratta spesso di un vantaggio di arbitraggio del lavoro una tantum, e molte organizzazioni hanno già realizzato queste efficienze, raggiungendo di fatto un "tetto" oltre il quale i costi e le prestazioni possono essere ulteriormente migliorati solo facendo le cose in modo diverso.

Ognuna di queste opzioni ha i suoi limiti. Nella continua ricerca dell'efficienza operativa, le aziende possono continuare a chiedersi come possono fare a:

- Evitare o rimandare l'elevato investimento di grandi programmi di trasformazione tecnologica mentre raggiungono i loro obiettivi operativi

- Sostenere la crescita del business senza l'aumento proporzionale dei costi operativi
- Derivare maggiore valore da operazioni già esternalizzate
- Sostenere l'innovazione di prodotti, processi e modelli di business e testare le idee senza costose nuove tecnologie

L'automazione di processo rappresenta un mezzo per raggiungere questi obiettivi, e ci sono due generi di strumenti in particolare di cui le aziende dovrebbero essere consapevoli: RPA e IA.

3.1 RPA E AI

I progressi tecnologici e le tendenze nel campo dell'Analytics, della Robotic Process Automation (RPA) e della Cognitive Intelligence (CI) stanno rapidamente rimodellando i modelli di business, migliorando la produttività e consentendo l'innovazione nel modo in cui le istituzioni finanziarie operano e conducono il business.

Secondo la società di ricerche di mercato Tractica, il mercato globale del software per l'intelligenza artificiale dovrebbe registrare una crescita massiccia nei prossimi anni, con ricavi in crescita da circa 9,5 miliardi di dollari nel 2018 a 118,6 miliardi entro il 2025, vedi grafico 3.1.

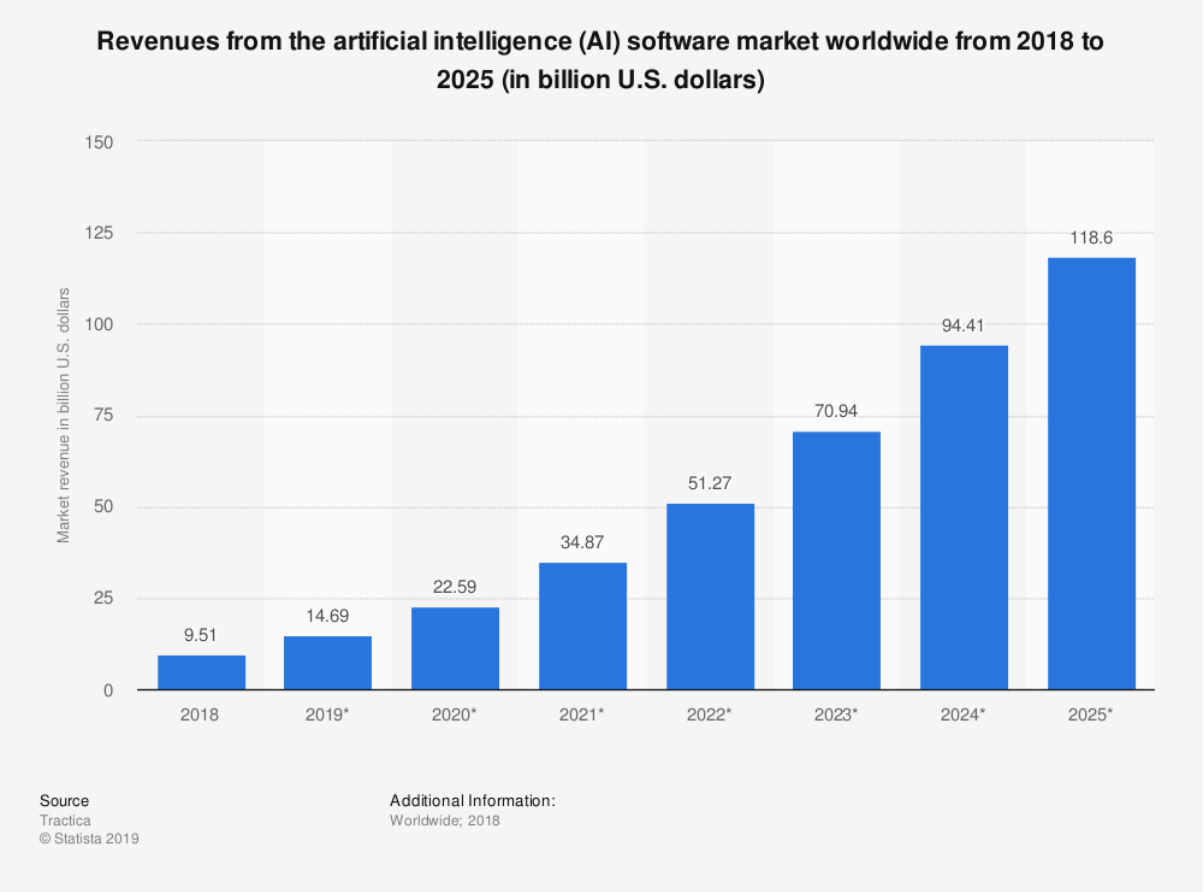


Grafico 3.1 Revenue AI

Molte aziende leader hanno adottato una o tutte queste tecnologie tra Machine Learning, RPA e Natural Language Processing per gestire le loro operazioni quotidiane.

La statistica seguente mostra a livello globale i tassi di adozione e di investimento sull'RPA per dimensione dell'organizzazione. Nel 2019, il 24% delle grandi organizzazioni ha adottato l'RPA, rispetto al 9% delle organizzazioni di piccole e medie dimensioni, vedi grafico 3.2.

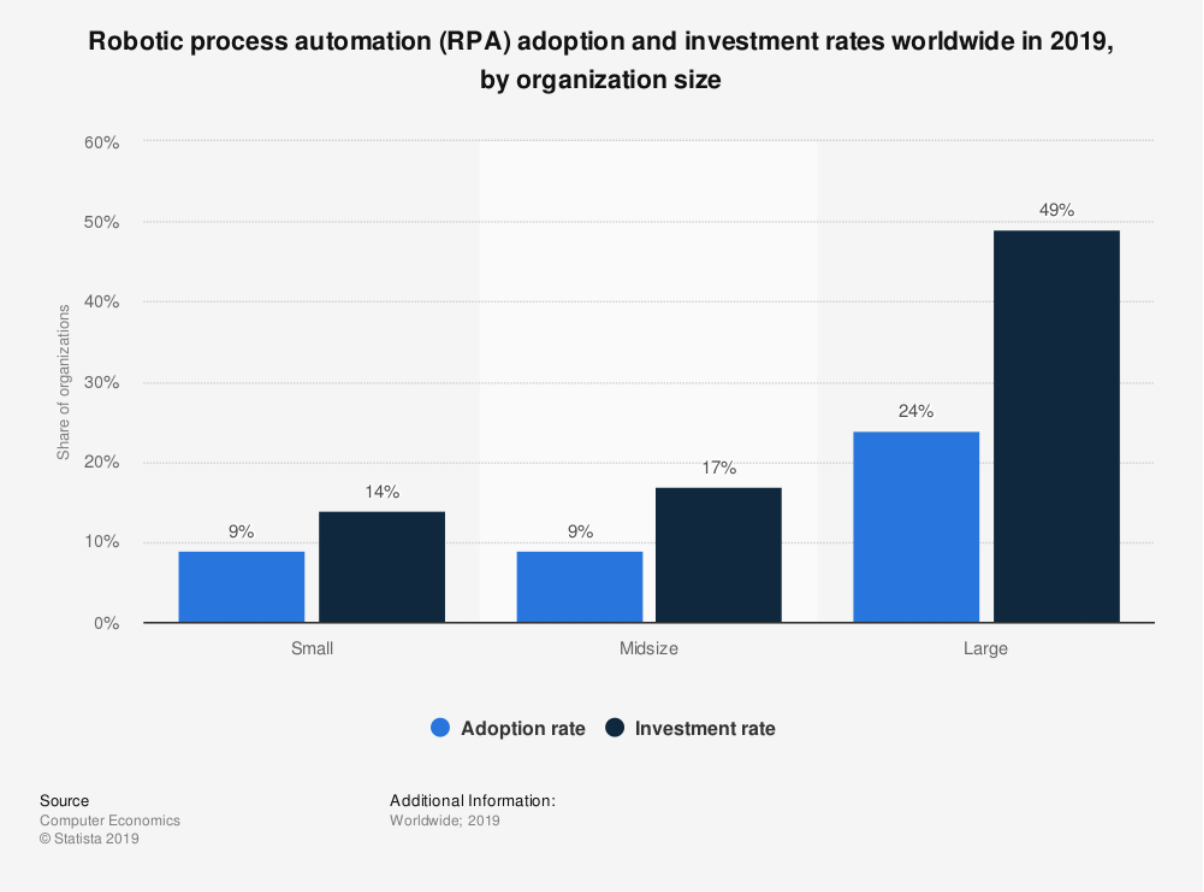


Grafico 3.2 RPA adoption and Investments

Secondo un sondaggio del 2018 tra i leader aziendali europei, il customer service e l'order processing sono state le aree su cui l'RPA ha avuto il massimo impatto. Il 43% degli intervistati, vedi grafico 3.3 ritiene che questa area di business sia diventata fortemente influenzata, insieme all'area finance, di tesoreria e della revisione contabile.

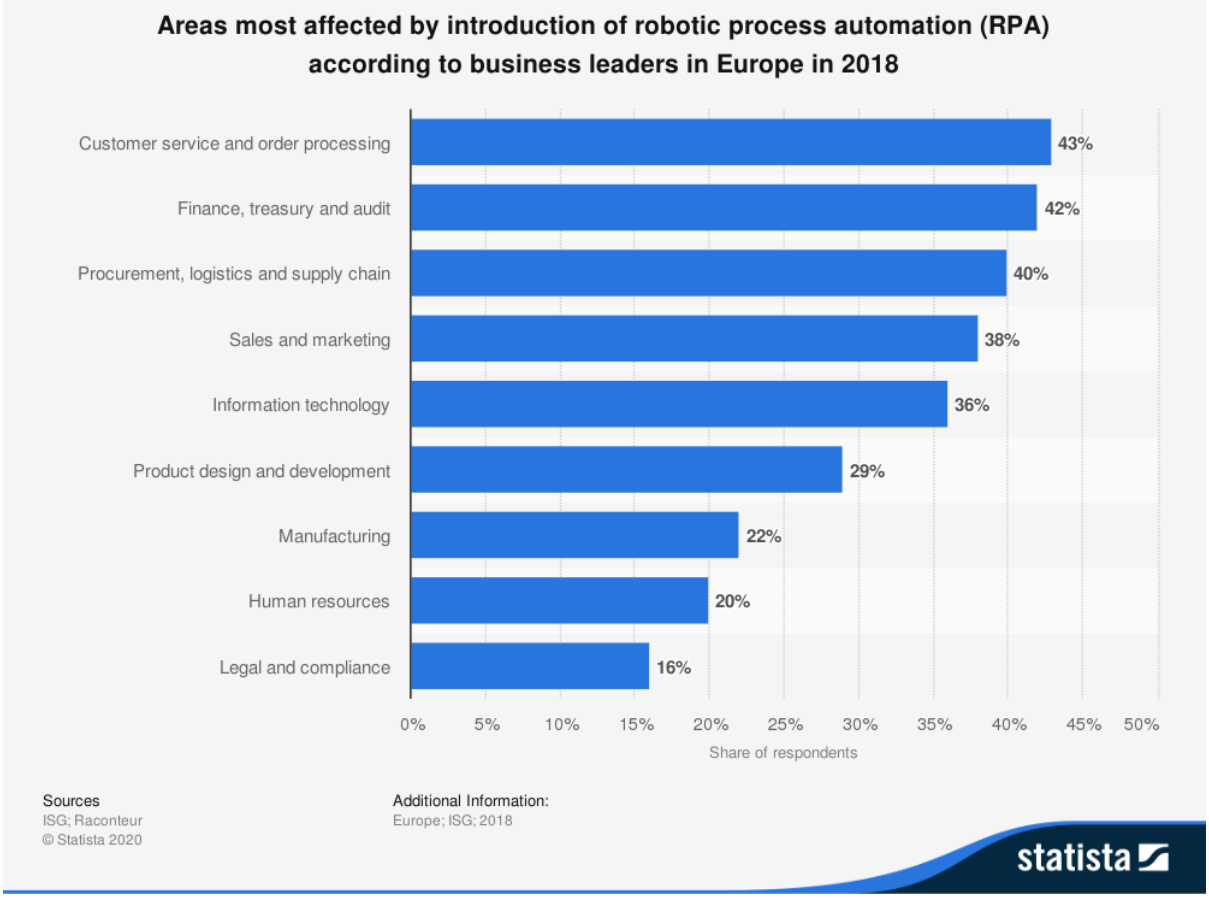
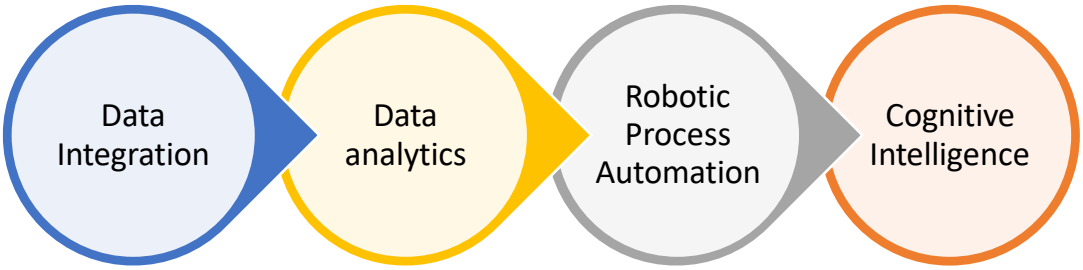


Grafico 3.3 Area of adoption of RPA

Le aziende di revisione contabile stanno infatti cercando di adottare tutte queste tecnologie con l'obiettivo di automatizzare parte dei propri processi per generare maggior valore e per permettere agli auditor di concentrarsi su attività più strategiche e non ripetitive.

L'obiettivo è quello di riuscire a digitalizzare parte della forza lavoro. Con il termine "digital workflow" si intende descrivere, infatti, le soluzioni automatizzate che possono svolgere dei processi all'interno di un'organizzazione, quali robot (RPA), chatbot, algoritmi e intelligenza artificiale.

Lo scenario comprende dunque un'ampia gamma di tecnologie digitali. Ad un'estremità ci sono i modelli predittivi e strumenti per l'integrazione e la visualizzazione dei dati e all'altro estremo sono le tecnologie avanzate con elementi cognitivi che imitano il comportamento umano.



Molte organizzazioni hanno già adottato la prima parte delle tecnologie digitali, avendo stabilito metodi di integrazione dei dati e programmi di Data Analytics per migliorare la valutazione del rischio con Predictive Analytics ovvero software che utilizzano modelli predittivi, e software per la Data Visualization che supportano le analisi e i processi di reporting.

Alcune organizzazioni hanno iniziato ad adottare l'RPA, ovvero rule-based systems che imitano il comportamento umano per automatizzare parte delle attività più ripetitive, insieme ad alcuni strumenti di CI, collettivamente noto come RPA&CI, per contribuire a migliorare l'efficienza e l'efficacia, espandere la capacità, aumentare la qualità e consentire una maggiore copertura di audit.

Nell'ambito della Cognitive Intelligence rientrano l'apprendimento automatico e l'intelligenza artificiale, ma ad ora è ancora limitato il numero di organizzazioni che hanno raggiunto questo livello di maturità digitale. Tuttavia, questa situazione sta cambiando rapidamente.

Oggi, i robot dominano la maggior parte della forza lavoro digitale e quindi la Robotic Process Automation è il fulcro principale della trasformazione della digital workflow.

3.2 Cos'è l'RPA nel dettaglio

L'RPA consiste nella configurazione di un SW che automatizza le attività e le procedure precedentemente eseguite dall'uomo attraverso le stesse interfacce utente. RPA interagisce con un sitema informatico come farebbe un essere umano, ma molto più veloce e ad un costo inferiore. Essa, infatti, mira a utilizzare un computer portatile per interagire con le applicazioni utilizzate in azienda (CRM, ERP, help desk, uffici del registro, altri lasciti) nello stesso modo in cui un essere umano utilizzerebbe le stesse applicazioni informatiche.

La tecnologia è capace di replicare operazioni come lancio di query, operazioni di copia/incolla dei dati, merging, button clicks. Risulta particolarmente utile per automatizzare attività umane ripetitive come lo scraping dei dati, l'inserimento dei dati in particolari form, l'azione in risposta a trigger basati su regole e l'acquisizione di immagini o di dati da esse. Esistono due tipi di RPA descritti di seguito.

Attended RPA

Essa prevede l'intervento umano durante l'esecuzione dei processi di automazione. Si parla di "bot assistito", in quanto opera sotto la direzione dell'utente. Si riporta un esempio di processo in figura 3.1.

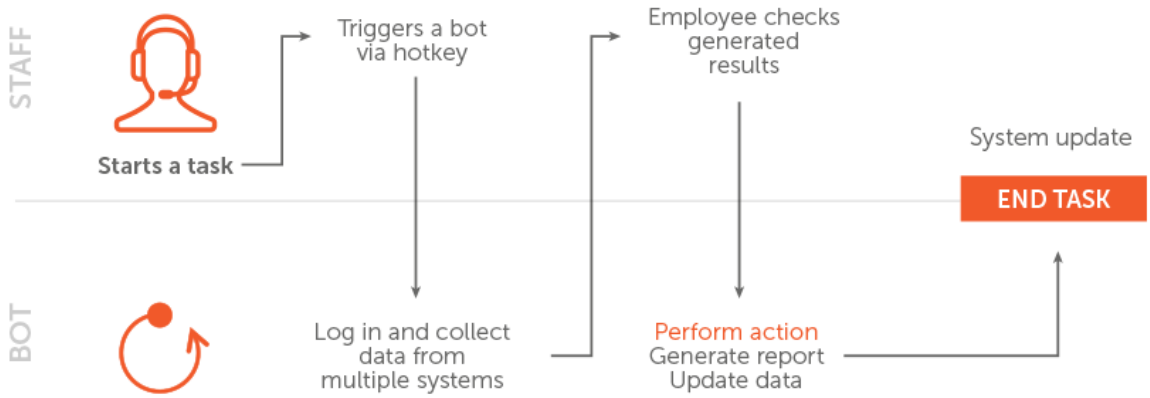


Figure 3.3 Attended RPA process Source Automation Anywhere

Il robot è “triggerato” dall’utente quando deve gestire attività ad alta intensità di dati. Il robot effettua allora il login e raccoglie i dati da diversi sistemi e database. L’utente allora esamina i risultati e autorizza il robot a generare il report o ad aggiornare i dati.

In questo modo l’utente ha il controllo, decidendo quando utilizzare l’automazione, ed è in grado di intervenire in caso di problemi.

Unattended RPA

Essa non prevede l’intervento umano durante l’esecuzione delle attività automatiche. I robot (figura 3.2) possono essere eseguiti sui server di un’organizzazione o su una macchina virtuale separati dalla user workstation, ad orari prestabiliti 24/7/365 e non richiedono l’attivazione dell’utente poiché le interazioni sono automatizzate in background. 29

Figure 3.4: Backoffice RPA Source Automation Anywhere

I bot di questo tipo sono spesso controllati da Center of Excellence dell’RPA (CoE) o sono guidati dall'IT in quanto possono utilizzare macchine virtuali per portare a termine il carico di lavoro. La significativa riduzione dei costi e l'aumento del ROI lo rendono ideale per le attività di back office.30

3.4 Applicazione RPA

[29] SIAV, *Robotic Process Automation,* https://www.siav.com/it/soluzioni-software/robotic-process-automation/
[30] AutomationAnywhere, Attended vs Unattended RPA, https://www.automationanywhere.com/solutions/attended-vs-unattended-rpa

L'RPA, in generale, può essere applicata sia nelle operazioni di back office come il controllo delle informazioni di anagrafica in entrata dei nuovi assunti, sia come supporto all'auditor nelle attività di front-end per confrontare più sistemi.

Il limite maggiore dell'RPA è che riesce a leggere solo dati strutturati quali database, excel, pagine HTML, ma non riesce a leggere dati non strutturati come pdf o immagini.

Inoltre, può essere applicata ad attività rule-based, legate a decisioni "if-then" riferite a set di istruzioni ben esplicite e non ambigue. Per cui è applicabile in processi con attività stabili nel tempo, molto ripetitive e time consuming che conviene automatizzare perché impegnano le risorse impedendo loro di svolgere attività di maggior valore.[31]

In figura 3.3 si riportano 15 task che possono essere automatizzati tramite RPA.

[31] NTT DATA CONSULTING, *LA ROBOTIC PROCESS AUTOMATION PER RIDURRE I COSTI DELLE OPERATIONS*

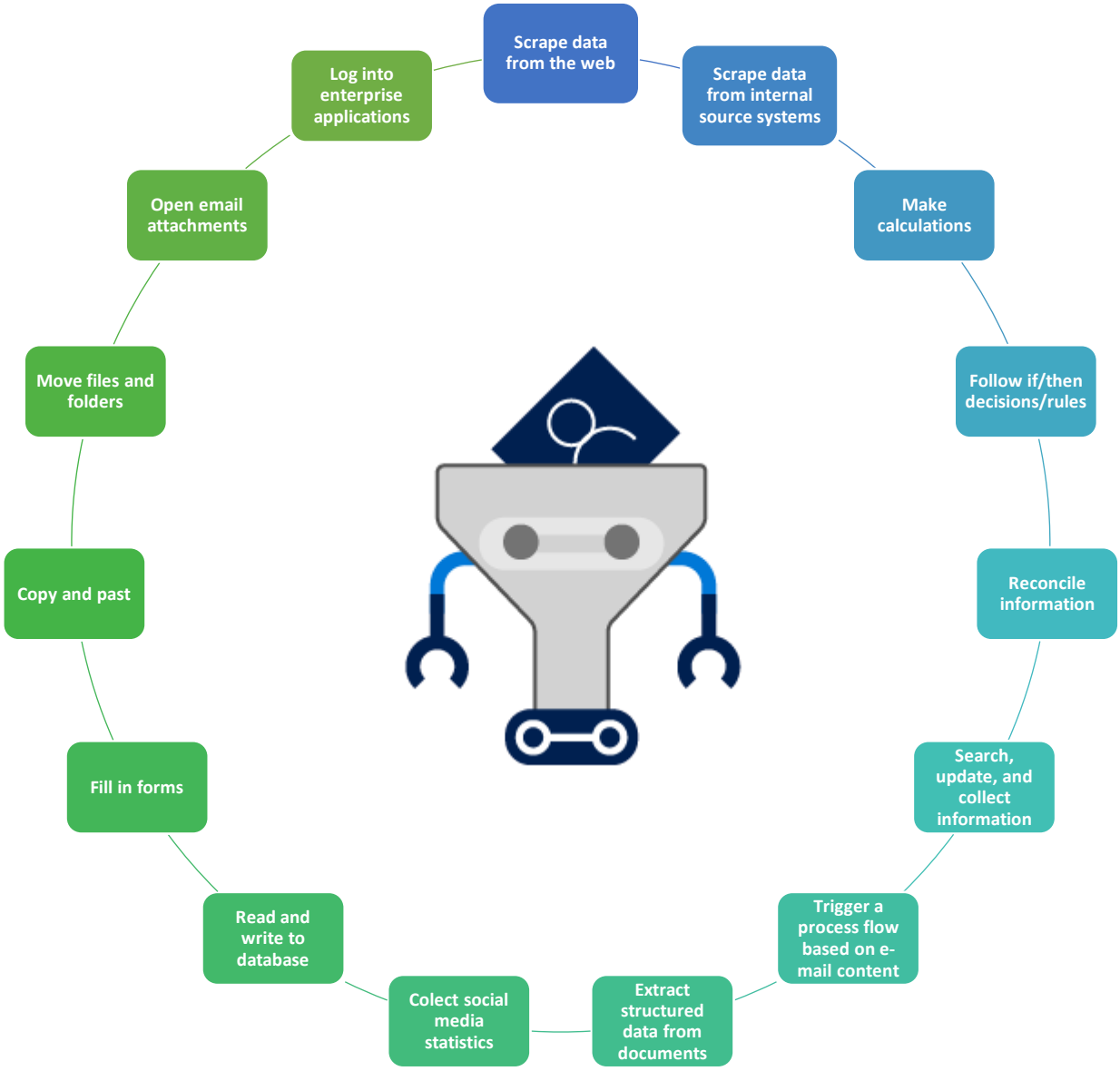


Figure 3.5 Attività performabili da RPA

3.5 RPA VS CI

Seppur avendo come comun denominatore l'automazione RPA e AI non sono sinonimi.

- Mentre gli strumenti RPA possono essere utilizzati solo per compiti di routine basati su regole, gli strumenti di IA possono portare valore migliorando i compiti non di routine che richiedono giudizio, intuizione, creatività, persuasione o la risoluzione dei problemi che però, d'altro canto, potrebbero essere molto difficili da automatizzare.

- Gli strumenti di IA sono tipicamente utilizzati per fornire un effetto leva alle funzioni esistenti, concentrandosi sull'aumento del valore piuttosto che sulla riduzione dei costi.

- Gli strumenti RPA possono essere implementati molto più velocemente degli strumenti di IA e richiedono tipicamente investimenti inferiori.

- Il mercato delle forniture RPA sta maturando rapidamente e ci sono diversi prodotti sul mercato che hanno dimostrato la loro efficacia. Gli strumenti di IA stanno migliorando rapidamente le loro capacità, ma nel complesso sono ancora in una fase nascente di sviluppo.

- Gli usi della IA sono potenzialmente senza limiti, ma anche più costosi. A differenza degli strumenti RPA, che sono molto ampi nella loro applicabilità, le soluzioni di IA richiedono una configurazione più estesa e un machine learning specifico per uno scopo aziendale molto più ristretto e per gli scenari complessi che può incontrare. Inoltre, le soluzioni di IA richiedono più tempo per essere implementate.[32]

Nella tabella 3.1 seguente sono riassunte le differenze tra le due tecnologie digitali.

[32] Deloitte, 2017, *Automate this The business leader's guide to robotic and intelligent automation*

Table 3.1 Differenze tra RPA e AI

	Robotic Process Automation	Intelligent Automation
Automatizza i compiti che sono…	Routine:Metodiche, Ripetitive,basate su regole fisse	Non di routine: Richiede una considerazione ponderata
In grado di…	Seguire le istruzioni	Arrivare alle conclusioni
L'applicazione è…	Più ampia: Può automatizzare qualsiasi processo adatto	Più stretta: L'applicazione dovrebbe essere mirata a fornire risultati significativi e perspicaci
Le offerte del mercato sono…	Mature	Emergenti
L'implementazione e i costi correnti sono tipicamente…	Bassi	Alti
I tempi di attuazione sono tipicamente dell'ordine di…	Settimane	Mesi

È da sottolineare che, a differenza di quanto avviene nel machine learning, l'RPA può gestire in modo ottimale processi ripetitivi ma non è in continuo apprendimento. Solo combinando RPA e AI si può ottenere l'*Intelligent Automation*, ovvero passare dall'automazione di processi specifici al funzionamento dei robot in veste di assistenti aziendali completamente cognitivi in grado di affrontare automaticamente tutti i tipi di attività ripetitive in tempo reale e alla fine liberare gli esseri umani da un lavoro che potrebbe altrimenti risultare banale e ripetitivo.[33]

I costi decrescenti dell'archiviazione dei dati e della potenza di elaborazione stanno consentendo rapidi sviluppi nel campo dell'Intelligenza Artificiale e la creazione di una nuova tipologia di tecnologie cognitive con capacità simili a quelle umane, come il riconoscimento dei documenti scritti manualmente, l'identificazione delle immagini e l'elaborazione del linguaggio naturale. Tramite *l'Intelligent Data Processing*, che utilizza algoritmi di Natural Language Processing su dati strutturati si possono svolgere attività quali la copia e l'incollatura dei dati tra le applicazioni, la riconciliazione e l'incrocio dei dati tra i diversi sistemi e, tramite algoritmi di Machine

[33] CUALEVA, *RPA e IA tra collaborazione e differenze*, http://www.cualeva.com/rpa-e-ia-tra-collaborazione-e-differenze/

Learning, la conduzione di processi decisionali di alto livello in punti chiave del processo aziendale.[34]

Se combinate con l'automazione robotica e la potente analitica, queste tecnologie cognitive possono formare soluzioni di "IA" che possono assistere direttamente le persone nell'esecuzione di compiti non di routine o addirittura automatizzare completamente tali compiti.

Inoltre, l'introduzione di RPA abbinata ad AI, a differenza di altri approcci, non costituisce una grande process disruption, in quanto non sostituisce l'IT tradizionale, per cui è più facile da applicare rispetto ad altri approcci. Infatti, il processo di automazione dell'IT può essere costoso e dispendioso in termini di tempo e può comportare complesse integrazioni e mappature dei dati tra i sistemi. L'RPA, invece, non richiede integrazioni tra i sistemi, perché operando a livello di User Interface Layer è in grado di automatizzare lavori rule-based senza compromettere l'infrastruttura IT sottostante, per cui risulta non invasiva.

Nella maggior parte delle organizzazioni, ci sono molti processi di routine eseguiti manualmente che non hanno la scala o il valore per garantire l'automazione attraverso la trasformazione IT, ma per i quali le macro e altri strumenti di automazione desktop di questo tipo sono troppo limitati per essere affrontati in modo efficace. L'RPA può aiutare a colmare questa lacuna, riducendo la "scala minima praticabile" dell'automazione dei processi rispetto ad altre opzioni tradizionali. Si veda la Figura 3.4.

[34] PWC, Robotic process automation: A primer for internal audit professionals

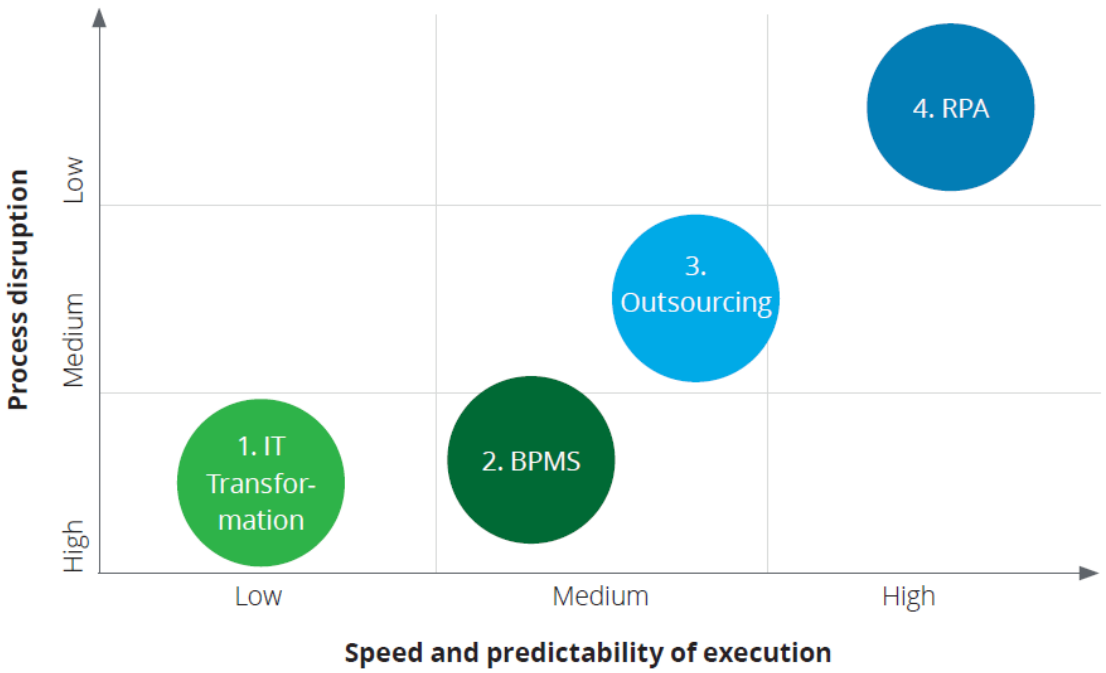


Figure 3.6 Confronto RPA con le altre trasformazioni IT, Deloitte

3.6 RPA: Lightweight o Heavyweight IT

Il confronto tra Lightweight e Heavyweight IT è stato sviluppato da Bygstad (2016), che ha introdotto questi termini per affrontare due tendenze del settore IT:

- la crescente dimensione e interconnettività dei sistemi IT
- la consumerizzazione ovvero il fenomeno in base al quale l'uso e lo stile delle tecnologie in ambiente lavorativo viene dettata, in sostanza, dall'evoluzione del profilo privato degli individui e dal loro utilizzo delle tecnologie personali[35].

L'IT Lightweight e Heavyweight non sono viste solo come approcci tecnologici diversi, ma due diversi regimi di conoscenza. Un regime della conoscenza in questo contesto significa un'unità che include una rete di attori, pratiche di lavoro, tecnologie e conoscenze condivise. Con l'Heavyweight IT si intende l'IT "tradizionale" o "mainstream", costituito dai sistemi e dai database tradizionali, che stanno diventando sempre più sofisticati e costosi grazie all'integrazione avanzata. La Lightway IT è il

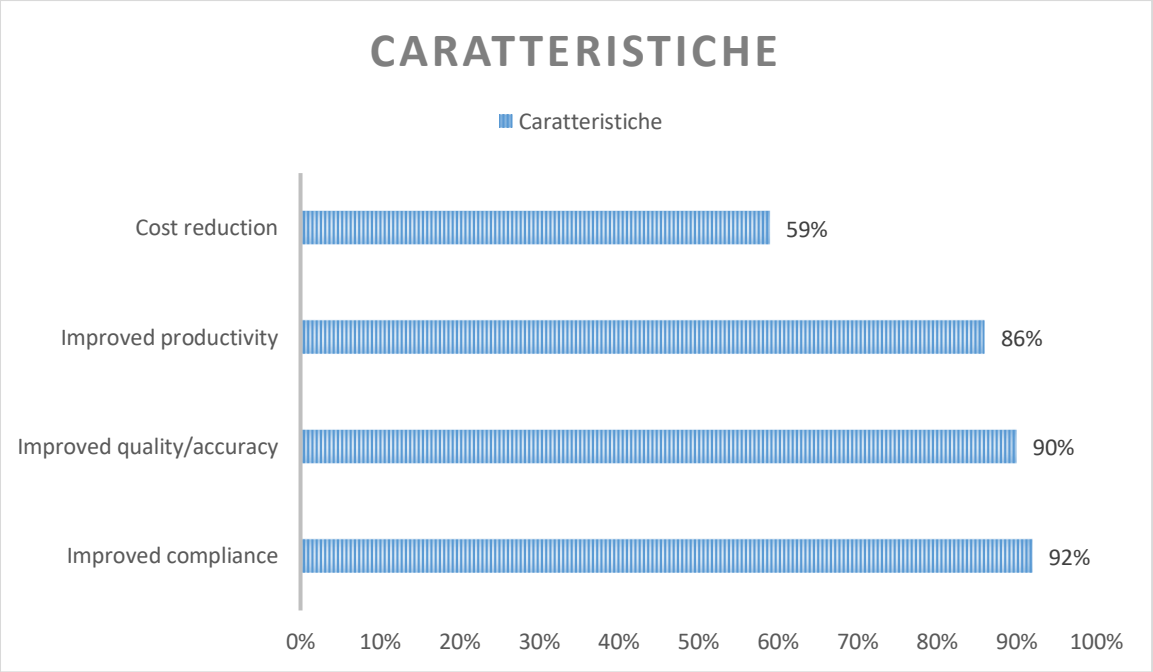
[35] Ilsole24ore, *Consumerization,* https://st.ilsole24ore.com/art/SoleOnLine4/100-parole/Tecnologia/C/Consumerization.shtml

nuovo paradigma delle applicazioni mobili, dei sensori e del bring-your-own-device, chiamato anche consumerizzazione o Internet-of-Things. caratterizzata dall'orientamento al business, la sperimentazione rapida e le soluzioni guidate dall'utente bypassando i reparti IT e utilizzando tecnologie facilmente disponibili (Bygstad, 2016). Un'altra differenza chiave in termini di lightweight e heavyweight IT è il grado della loro invasività. Le soluzioni lightweight utilizzano spesso il presentation layer e non modificano la struttura profonda sottostante del sistema o delle architetture di dati, mentre le soluzioni heavyweight agiscono sui livelli di accesso ai dati o di business logic (Willcocks et al., 2015a).

L'RPA operando solo a livello di Presentation Layer può essere classificata come lightweight IT, quindi apporta benefici perché non richiede l'integrazione dei sistemi ma necessita di un corretto supporto da parte dell'IT. Il livello di "invasività" dipende come l'organizzazione decide di implementarla.36

3.7 Vantaggi di applicazione dell'RPA

Secondo lo studio di Deloitte, *New Digital Riks*, *RPA and IoT* (settembre 2019) l'RPA consente di raggiungere i seguenti target:



[36] Bendig Bygstaf, *The Coming of Lightweight IT, 29/05/2015,*
https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1021&context=ecis2015_cr

- RIDUZIONE DEI COSTI: è stato stimato che i robot riescono a compiere lavoro equivalente al 20% FTE. La riduzione dei costi avviene dunque in termini di riduzione della forza lavoro che viene sostituita in parte da capitale. Sebbene infatti il costo del software sia elevato, il ritorno sull'investimento è veloce con PayBack stimati nella maggior parte dei casi di un anno.
- AUMENTA LA PRODUTTIVITA': Il numero di transazioni che l'RPA può effettuare in un'ora superiore a quello di un essere umano, quindi l'azienda può gestire più velocemente un maggior numero di dati e informazioni, raccogliendoli laddove non era fattibile per gli esseri umani. Pertanto, una più ampia portata della raccolta e dell'analisi dei dati porta ad approfondimenti più completi e completi. Tracciando i processi, infatti, l'RPA consente di scovare le lacune e implementare le misure per consentire un'ulteriore ottimizzazione. Nel frattempo, i dipendenti possono concentrarsi su analisi più sofisticate e su attività di maggiore valore, che portano a un migliore processo decisionale. Modificando i compiti delle risorse umane, ovvero automatizzando i compiti ripetitivi che spesso sono svolti con minore attenzione le aziende possono ottenere lo svolgimento di task significativi creando maggiore valore.
- AUMENTA LA QUALITA': L'RPA razionalizza, standardizza e ottimizza i processi, migliorando la qualità con un alto grado di precisione e operando 24x7. Inoltre, l'automazione riduce il rischio di errore dovuto alla natura manuale delle attività e all'eliminazione dei compiti a basso valore aggiunto. L'RPA introduce infatti maggiore precisione nelle operazioni e rende i processi monotoni privi di errori. Tuttavia, richiedono test, addestramento e governance per ottenere i risultati desiderati.
- MIGLIORA LA CONFORMITA' ALLE NORMATIVE: Per le aziende la conformità alle normative, come il rispetto del GDPR è molto importante. Un processo RPA completamente automatizzato consente loro di tracciare ogni passaggio documentandolo sistematicamente, aiutandole a essere allineate alle normative di settore e di revisione. Infatti, piattaforme tecnologiche RPA, utilizzano strumenti di specificazione basati su modelli che mostrano graficamente come i robot interagiscono con i sistemi e generano anche dati operativi che possono essere analizzati e compresi dai non specialisti. Durante il processo di automazione, le azioni dei robot software RPA vengono salvate

in un registro dove possono essere esaminate e monitorate in qualsiasi momento. Ciò significa che le aziende hanno un maggior grado di supervisione e controllo sulle proprie operazioni e i dipendenti possono affrontare più facilmente i problemi di conformità se si presentano, per cui aumenta l'auditabilità. [37] Tramite l'RPA non si rende più necessario campionare per effettuare le verifiche, riducendo il sampling bias. Infatti, attualmente si campiona perché non ci sono abbastanza risorse per controllare ogni azione intrapresa. Con l'RPA, di conseguenza, non solo vengono eliminati errori di distorsione introdotti da un campione limitato, ma il processo di revisione stesso può cogliere azioni non conformi che sarebbero state trascurate dai revisori che avrebbero esaminato solo un campione limitato. Inoltre, guardando nello specifico al rispetto del GDPR, un elemento significativo dell'implementazione quotidiana del GDPR ruoterà attorno ai day-to-day tasks come la ricerca di dati personali in risposta a una richiesta di accesso da parte di un soggetto, l'esecuzione della cancellazione dei dati e la preparazione di rapporti sui dati personali. Tecnologie RPA hanno il potenziale per facilitare questo lavoro, minimizzando i costi e massimizzando la qualità e la tempestività delle risposte. Dunque, l'attended RPA guida gli utenti in tempo reale e in modo contestuale, per garantirne una maggiore conformità alle normative, ai modelli e alle procedure specifiche all'interno dell'azienda.[38]

3.8 Applicazione RPA all'audit

Per il ruolo che svolgono, le funzioni di audit dovrebbero contribuire in modo proattivo all'innovazione responsabile. Devono essere in grado di valutare rapidamente l'impatto completo dei progressi tecnologici e poi fare perno su ogni nuova innovazione per comprendere appieno il modo in cui l'innovazione sta agendo per cambiare il profilo di rischio dell'organizzazione.

È importante infatti, al fine della revisione, che l'audit abbia una prospettiva sui rischi che le nuove tecnologie comportano e sui controlli in atto per gestire adeguatamente

[37] Uipath, *How Robotic Process Automation Powers Bulletproof Legal Compliance,* https://www.uipath.com/blog/rpa-improves-legal-compliance
[38] *ENGINEERRING, ROBOTIC PROCESS AUTOMATION* https://www.eng.it/resources/whitepaper/doc/rpa/RPA_whitepaper_ita.pdf

questi nuovi rischi, al fine di valutare le procedure attuate dai clienti. È compito dell'audit anche fornire consulenza su come l'organizzazione dovrebbe sfruttare le nuove tecnologie e formulare raccomandazioni sull'ambiente IT del cliente auditato.

Allora, le funzioni di audit possono servire in questa preziosa funzione solo se sono esse stesse innovatrici, o altrimenti, il valore apportato diminuirà.

Alcune funzioni di audit si stanno orientando proprio verso questo futuro guidato dalla tecnologia. Stanno già fornendo consulenza per clienti che utilizzano RPA e IA, devono quindi avvalersi di strumenti, competenze e metodi innovativi per fornire garanzie.

La direzione in cui si stanno muovendo è l'utilizzo di strumenti di estrazione dati e RPA per migliorare la convenienza e la copertura dei loro audit, e l'analisi, l'intelligenza artificiale e l'apprendimento automatico per offrire alle organizzazione intuizioni innovative e a valore aggiunto.

3.8.1 Stato attuale di automazione delle attività da parte delle società di revisione

Come illustrato in precedenza, le attività di audit sono spesso ripetitive e richiedono elevati sforzi nella raccolta dati e nell'analisi degli stessi data la loro grande quantità. Per velocizzare tali attività gli auditor utilizzano diversi strumenti informatici di supporto, come mostrato in tabella 3.2.

Tabella		
Un confronto tra gli strumenti di automazione per le attività di audit		
Tools	Esecuzione del tool	Audit task
Excel Macros	Rules-Based Functions	Reconciliations
IDEA	Calculations	Analytical Procedures Internal Control Testing Detail Testing (Attribute Match)
Python	Rules-Based Functions	Reconciliations
R	Calculations Web Scraping	Analytical Procedures Internal Control Testing
ACTT	Exporting Data	Input: Collection of Data
RPA Vendor Tools, Such as UiPath and Blue Prism	Importing Data Exporting Data	Detail Testing (Attribute Match) Input: Collection of Data Output: Compilation of Audit Test Results

Table 3.2 Confronto tool di automazione

Excel rappresenta il tool di base per effettuare le analisi e le riconciliazioni attraverso macro preimpostate, ma risulta molto macchinoso e richiede una grossa interazione dell'auditor.

Caseware IDEA è un tool di supporto specifico alle attività di auditing. Esso permette di importare set di dati di diverso tipo, strutturati e non strutturati (xls, pdf, txt..) leggerli da diverse sorgenti come ODBC e SAP e trasferirli in dashboard che semplificano l'analisi degli stessi, velocizzando il monitoraggio, l'identificazione di trend e di outliers. La visualizzazione può mostrare le transazioni che fluiscono attraverso il flusso di lavoro e agevolare l'individuazione delle aree che possono richiedere un'indagine più approfondita dal punto di vista del rischio e dei controlli o dell'efficienza operativa. IDEA riperforma un tipico processo ETL (Extract Transform Load) ma richiede l'integrazione di script di Python per l'esecuzione di test specifici ripetuti.[39]

Python e R sono linguaggi di programmazione che permettono di effettuare analisi molto più avanzate rispetto ai primi due tool presentati. Tramite essi è possibile non solo scaricare dati in automatico da diverse sorgenti non strutturate ma anche creare test ripetibili che riducono il tempo di analisi tramite l'analitica avanzata. Tuttavia, il loro utilizzo non è banale in quanto richiedono personale molto skillato in ambito IT.

L'ACTT, Automated Controls Testing Tool, è un tool sviluppato da Deloitte è può essere considerato come un primo tool di RPA per il supporto specifico all'IT Auditor, usato per estrarre i dati dall'ambiente IT dei clienti auditati. Esso si basa su una web-application architecture con un SQL Server database che effettua il back-end processing. L'ACTT è in grado di prelevare dati dal sistema ERP del cliente, processarli ed esportare i risultati su Excel.

I risultati che genera sono report relativi all'analisi della SOD (Segregation of Duties), Sensitive Access e Configured Control (GITC).

[39]IDEA, *The Trusted Tool for Data Analysis,* https://idea.caseware.com/products/idea

L'estrazione dei dati avviene a seguito dell'installazione del tool nell'ambiente IT del cliente, che non modifica in alcun modo il sistema, ma si limita ad avviare delle queries in sola lettura finalizzate all'estrazione dei dati propedeutici al test dei controlli.

Il limite più grande dell'ACTT è che si applica solo a sistemi standard, quali:

APP-DB-OS	Supported by ACTT – Release 15 (Summer 2018)
SAP ERP	X
Oracle EBS ERP	X
PeopleSoft ERP	X
JD Edwards	X
Oracle	X
HANA	X
MS-SQL	X
AIX	X
Solaris	X
Linux	X
HPUX	X
Windows OS and AD	X
AS400	

L'auditor ha il compito allora di:

- settare le regole nel tool per l'estrazione dei dati di interesse del cliente per il test dei controlli;
- effettuare l'analisi dei dati estratti e la formalizzazione dei test;
- fornire il *Judgment* sull'efficacia dei controlli.

L'ACTT si limita a riportare i risultati dei test senza formalizzazione e senza giudizio finale. Tuttavia riduce al minimo il tempo di raccolta dati del cliente che spesso è la causa principale del ritardo delle attività. L'ACTT può essere considerato come un tool di attended RPA.

Uipath e Blue Prism sono tra i primi tool di RPA&CI per l'automazione di Finance e Accounting. Essi utilizzano l'Intelligent Optical Character Recognition per leggere dati

non strutturati, il Machine Learning e il Natural Language Processing per eliminare qualsiasi azione manuale e quindi permettere all'auditor di concentrarsi su attività diverse e più strategiche. Una customizzazione degli stessi permetterebbe di raccogliere dati, testarli e generare in automatico form compilati con i risultati dei test di auditing. Le compagnie tecnologiche sviluppatrici di Uipath e Blue Prism hanno attivato partnership con le maggiori società di consulenza con l'obiettivo di creare un'automazione apposita per i loro sistemi, ma sono ancora in fase di implementazione.

3.8.2 L'impatto del bot sull'audit

L'RPA rappresenta un valore aggiunto per l'automazione delle attività di controllo, sia in termini di esecuzione del controllo stesso che di verifica dei relativi output. Tali attività consentono di aumentare l'efficienza della gestione del processo di controllo e di ridurre lo sforzo richiesto per l'esecuzione delle analisi.

Le attività che può effettuare il bot sono:

1. Raccogliere ed elaborare i dati, i bot possono estrarre dati da varie fonti su base periodica, aggregare e presentare i dati in un formato predefinito e convalidarli in base a un elenco di regole di business
2. Inviare notifiche in caso di rilevamento di eccezioni, in caso di discrepanze o non conformità, le email saranno automaticamente inviate alla parte responsabile per ulteriori indagini per risolvere i problemi.
3. Eseguire attività di controllo, seguendo procedure specifiche, valutando il controllo per determinare se ha funzionato efficacemente per ogni progetto. Ad esempio, il bot può eseguire test indipendenti in base ai requisiti normativi e di audit interno, e registrare le segnalazioni quando vengono identificati i problemi.
4. Eseguire la pianificazione del controllo, eseguire i test e fornire la supervisione. Se un controllo è fallito, il robot può pianificare automaticamente la prossima valutazione e avviare le attività di test. Il bot può anche generare report per la gestione di problemi (ad esempio, se il controllo continua a fallire).

Tuttavia, ci sono dei rischi da considerare annessi all'utilizzo dei robot come presentati in tabella.

Ruolo robot	Attività svolta	Rischi legati al bot	Temi da considerare
Control Executor	Il robot può (parzialmente) eseguire un controllo come l'approvazione del flusso di lavoro sulla base della documentazione disponibile o la creazione/cancellazione degli utenti sulla base delle informazioni disponibili nello strumento di ticketing.	Per impostazione predefinita, gli account dei bot non sono utenti del sistema e quindi è necessario riflettere a sufficienza su come proteggere il Bot da accessi non autorizzati e modifiche.	**Protection of the Bot**
Control Tester	I robot possono estrarre, interpretare e concludere sui dati per concludere sull'efficacia dei controlli sia manuali che automatici.	I cambiamenti nel panorama informatico non solo influenzano l'applicazione a cui il cambiamento è destinato, ma potrebbero anche influire sul funzionamento del robot.	**Changes in IT landscape**
Report generator	I robot possono estrarre, interpretare e concludere sui dati per concludere sull'efficacia dei controlli sia manuali che automatici.	Poiché i bot possono eseguire controlli manuali e automatizzati, il cliente deve implementare un numero sufficiente di GITS per proteggere sia i bot che la logica del report.	**General IT Controls on RPA solutions**

Table 3.3 Rischi legati all'utilizzo del bot

3.8.3 Rischi

I robot non hanno "buon senso", quindi se un difetto nel processo di gestione dei robot dell'organizzazione permette a un errore evidente di insinuarsi nelle istruzioni fornite ai robot, essi seguiranno comunque le istruzioni alla lettera - e replicheranno l'errore centinaia o migliaia di volte fino a quando qualcuno non lo noterà. Oppure, se c'è un cambiamento di processo aziendale ma il robot non è stato modificato per riflettere quel cambiamento, esso può non eseguire le attività o introdurre imprecisioni. Altro rischio potenziale è l'accesso non autorizzato a un robot, che potrebbe essere alterato o usato per condurre trattamenti non autorizzati.

I Chief Audit Executives (CAE) e i loro team devono allora capire i rischi connessi all'utilizzo dell'RPA, stabilire la governance di RPA e dei controlli rilevanti che dovrebbero aiutare in modo efficace a mitigare i rischi.

La gestione del rischio per le attività svolte con l'RPA prevede di:

- Assicurare il corretto funzionamento dei bot
- Prevenire l'uso non autorizzato
- Prevenire il bypass dei controlli aziendali e IT
- Regolare le modifiche al software e agli script RPA
- Affrontare i rischi per la sicurezza
- Garantire la conformità alle leggi e ai regolamenti

Aree di rischio:

Maintenance e operation: al pari di un dipendente, i robot richiedono una guida per svolgere le attività desiderate. Anche se i robot sono configurati alla perfezione in un dato istante temporale sulla base di definiti requisiti di business, un'architettura più ampia e cambiamenti di sistema possono influire pesantemente sulle prestazioni previste. Inoltre, la mancata creazione di agili meccanismi di supervisione e controllo può portare a inefficienza operativa quando i bot o gli algoritmi richiedono modifiche, aggravata dal fatto che gli effetti degli errori di elaborazione possono essere amplificati dal bot.

Financial: gli errori legati ai bot possono avere un impatto negativo sull'integrità dei rapporti finanziari interni ed esterni e un'implementazione o un'automazione impropria dei processi può comportare perdite finanziarie per l'organizzazione.

Regulatory: gli errori relativi ai bot possono influenzare la validità e l'accuratezza dei processi di reporting normativo. Inoltre, manca ancora una guida chiara da parte degli enti normativi in merito ai principali standard per l'automazione e la progettazione di algoritmi per cui l'organizzazione dovrebbe essere attenta a regolarizzare i bot e gli algoritmi in quanto potrebbero inavvertitamente violare le leggi.

Technology: Un'anomala attività dei bot può avere un forte impatto sulle funzioni dei sistemi IT esistenti e inoltre potenti algoritmi possono avere un impatto negativo su altri elementi critici.

Cybersecurity: l'abuso di accessi privilegiati, i diritti di accesso mal gestiti e la divulgazione di dati sensibili possono impattare sull'integrità e sull'affidabilità dei processi aziendali gestiti dall'RPA.

Organizational: la sostituzione o la riqualificazione di FTE può avere un impatto negativo sul morale dei dipendenti e il disallineamento tra i gruppi può portare a lacune nei ruoli e nella responsabilità.

Reputational: algoritmi senza controlli adeguati possono indurre un rischio significativo per la reputazione. La comunicazione e il coordinamento possono essere necessari tra il team di gestione con i fornitori e i clienti per garantire che l'attività dei bot non crei problemi operativi o di marchio/ reputazione.

3.8.4 Impatto su organizzazione

Per sfruttare appieno il potenziale dell'IA e della robotica, le aziende devono aumentare le competenze delle persone che lavoreranno a fianco dei robot, nella forza lavoro 'aumentata', consentendo loro di fornire attività di maggior valore.

In una prima fase, come in tutti i processi di automazione, ci sarà una riduzione del personale, per la sostituzione di lavoro con capitale. Le figure meno skillate tecnologicamente saranno sostituite non appena si giungerà a un livello di accuratezza della macchina affidabile e sarà necessario sostituirle o riformarle sulla nuova tecnologia.

Se si costruiscono internal capabilities per l'automazione, si deve considerare quale figura sarà responsabile di:

- valutazione della mappatura e della priorità dei nuovi processi di automazione;
- sviluppo e test dei lavori automatizzati;

- gestione e monitoraggio dei robot software mentre operano.

Infatti, né le soluzioni RPA né quelle di IA riescono a replicare appieno il ragionamento umano. I robot software RPA imitano il comportamento degli esseri umani nel modo in cui interagiscono con le interfacce utente delle applicazioni, ma devono seguire istruzioni altamente metodiche e una semplice logica condizionale.
Si rende quindi indispensabile avere delle figure che si occupino del monitoraggio dell'attività dei robot tramite dashboard e report, con funzionalità di controllo delle versioni e gestione delle release per supportare la definizione dei processi e l'implementazione oltre i confini organizzativi.
Ma non sono richieste solo competenze specialistiche specifiche della RPA: sono essenziali anche la gestione del progetto, dei processi e le competenze di gestione del cambiamento.

Per la gestione di tali attività, Forrester prevede la creazione di 14,9 milioni di nuovi posti di lavoro nei soli Stati Uniti entro il 2027.

Le principali figure che saranno richieste sono:

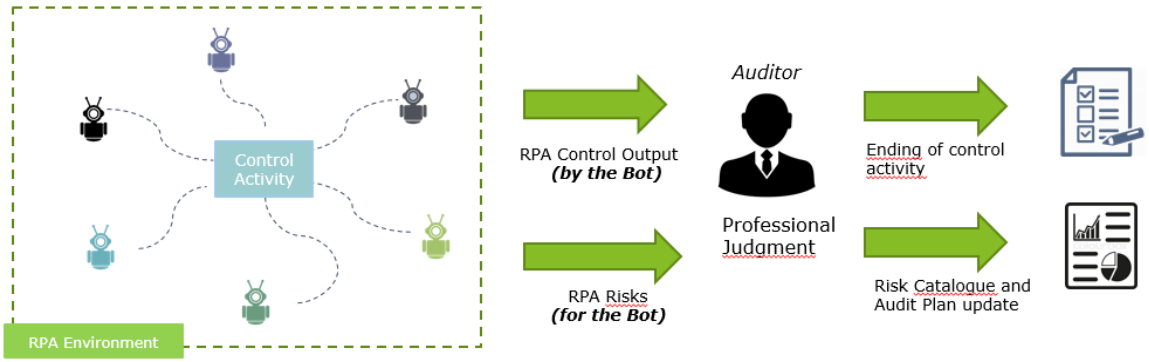
- Data scientists
- Automation specialists
- Content curators
- RPA architects
- Process developers specificano le istruzioni dettagliate che i robot devono eseguire e le "pubblicano" nel robot controller repository
- Il robot controller viene utilizzato per assegnare i lavori ai robot e per monitorare le loro attività.

Sono dunque necessari nuovi modelli organizzativi e operativi e una questione chiave è dove collocare i team di attuazione dell'RPA. Mentre questioni come gli obiettivi, il metodo, e l'assicurazione della qualità possono essere gestiti a livello centrale per l'intera impresa, la proprietà dell'implementazione RPA sarebbe meglio distribuita a livello di business unit o funzione. Molte organizzazioni sviluppano un Automation Center of Excellence (unità aziendali o centri di eccellenza) per facilitare la formazione e la condivisione delle conoscenze e delle migliori pratiche.

Tuttavia, per la maggior parte delle organizzazioni, l'implementazione comporta la collaborazione con un partner terzo dedicato, spesso per fornire consulenza e competenze che sono scarse nella propria organizzazione. Questo supporto va da soluzioni turn key alla collaborazione per la creazione di team interni ad alto livello di competenze sull'RPA.

3.8.5 Nuova figura auditor

L'evoluzione della RPA sta gradualmente trasformando il business, portando ad una revisione dei vari ruoli aziendali, come il revisore dei conti. Grazie all'automazione, l'auditor viene liberato dalle attività di controllo di routine e dalle lunghe attività di controllo, permettendogli così di concentrarsi su tutti quei compiti che richiedono giudizio e competenza professionale per la loro esecuzione.



CAPITOLO 4 – PROGETTO APPLICATIVO SU SOCIETA' DI REVISIONE X

4.1 Esposizione del processo e del problema

A seguito del tirocinio svolto presso la società di revisione GUASIM Milano S.p.A. si è sviluppata un'analisi critica del processo di business della stessa, con problematiche comuni alle altre società di consulenza.

Il metodo di analisi prevede inizialmente di andare a descrivere gli step del processo di supporto audit, dal primo contatto con il cliente alla consegna finale del report da allegare alla Nota integrativa della società.

In seguito si analizzano le criticità del processo, andando a riportare dati interni della società di revisione e analisi ottenute tramite questionario ai dipendenti.

Si procede infine a sviluppare un progetto di automatizzazione di parti del processo, analizzando i vari step che potrebbero essere "robotizzati" con l'RPA supportati da una valutazione economica e una proposta riorganizzativa della stessa professione.

4.1.2 Descrizione degli step del processo attuale

L'attività dell'IT Auditing si compone di sei attività principali come mostrato in Figura 1:

1) Acquisizione del cliente oggetto di revisione;
2) Kick off con il cliente e raccolta preliminare dei dati;
3) Raccolta documentazione a supporto delle analisi, da remoto e/o tramite incontro diretto con il cliente per testare i controlli effettuati da esso sui sistemi informativi;
4) Formalizzazione (design and operation effectiveness) delle evidenze ricevute con individuazione di eventuali deficiency;
5) Review da parte del partner, del manager e del senior consultant;
6) Chiusura progetto con consegna report al cliente;

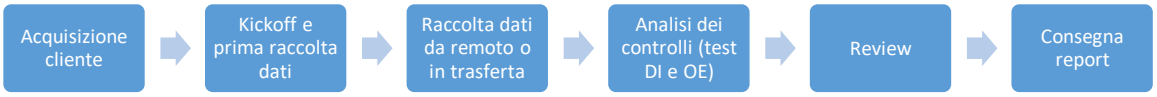


Figure 4.1 Processo IT Auditing

La fase 1 di acquisizione del cliente, prevede il contatto tra il partner ed il cliente, con uno o più incontri tra le parti per stabilire le attività di controllo da effettuare, le tempistiche e il budget di progetto (prima stesura del Planning Memo del progetto).

La fase 2 prevede l'incontro tra cliente, manager e senior consultant, per iniziare ad organizzare la parte operativa del progetto. Durante il kickoff, si procede ad ottenere una visione generale dell'ambiente IT con l'individuazione di tutti i suoi costituenti quali applicativi, database e sistemi operativi (Understanding of IT Environment). In questa sede si indaga sui sistemi di controlli interni IT applicati dalla società, ovvero la Mappa Applicativa dei controlli e i rischi che mira a coprire (Risk Assessment). È effettuata una prima raccolta di dati generali.

Nella fase 3 si ha la raccolta completa dei dati necessari alla redazione dei GITC (General IT Controls), dei controlli automatici (ITAC), delle IUC e delle IPE e delle interfacce se previste. Essa può prevedere l'incontro diretto dell'analyst e del consultant con il team IT della società auditata nel caso in cui il budget rientri nel range medio grande, ovvero budget>20K€ (circa il 30% dei clienti). È necessario l'incontro diretto se devono essere effettuati controlli automatici, in quanto si riferiscono a specifiche applicazioni informatiche e a singole transazioni che avvengono all'interno dell'ecosistema informativo aziendale. Infatti, essi variano a seconda del numero di

interfacce tra i diversi applicativi presenti e della procedura di fatturazione, gestione ordini e rimanenze adottata.

Tale fase ha una durata molto variabile, in quanto dipende dalla disponibilità dei referenti IT della società auditata e dalle tempistiche di invio da parte degli stessi della documentazione/evidenze richieste dal team di audit. Per questa ragione, spesso si sovrappone alla fase successiva di analisi delle evidenze e richiede continui solleciti via mail o tramite call.

La fase 4 è quella più operativa e incisiva sulle tempistiche del progetto, in quanto prevede tutta l'analisi della documentazione ricevuta, il test dei controlli effettuati dalla società e la formalizzazione del lavoro. In questa fase sono svolti i GITC, ITAC, IUC, IPE, analisi interfacce, JET e APP se previste.

Nella fase 5 avviene la review del lavoro svolto da parte del senior consultant del manager ed infine dal partner. Essa può avere esito positivo o negativo; nel secondo caso il lavoro deve essere corretto e riperformato.

Nella fase 6 si ha un incontro diretto o meno tra il manager, il partner e la società auditata per la consegna dei report sviluppati sulla mappatura dei controlli e quindi la chiusura del progetto.

4.1.3 Criticita' del processo:

- STAGIONALITA' DOMANDA

La revisione contabile si compone di tre macro fasi, la pianificazione (step 1, 2), l'analisi (step 3, 4, 5) e la conclusione del progetto (step 6).

- Nei mesi di giugno, luglio, agosto e settembre si svolgono i kickoff con i clienti e quindi la fase di pianificazione della attività. Questo è il periodo "scarico" di lavoro in quanto lavorano principalmente partner, manager e senior consultant.
- Nei mesi da ottobre a dicembre si svolge la fase *preliminary* di testing sui controlli, nel periodo che precede quindi la chiusura dei bilanci (31/12).
- Nei mesi che vanno da gennaio ad aprile si svolge la fase *final* di testing sui controlli, ovvero nel periodo che va dalla chiusura alla presentazione del bilancio (30/04 o in casi particolari 30/06).

Per la conclusione delle analisi è importante rispettare la data di Opinion, cioè il giorno in cui l'Audit si deve esprimere sul bilancio della società con l'emissione della Nota che poi essa dovrà allegare al proprio bilancio.

L'IT Audit ha l'obbligo di esprimersi sull'efficacia dei controlli, ovvero sulla presenza o meno di deficiency entro la data di Opinion, ma ha ulteriori 40 giorni per completare la formalizzazione. Per tale ragione, alcuni progetti sono conclusi solo a fine maggio.

Per alcuni clienti quotati in borsa americana, la data di Opinion corrisponde con la chiusura del progetto stesso. In questo caso, sono permesse minime modifiche e il tutto deve essere tracciato all'interno di un apposito file in cui sono indicate le modifiche apportate, la data, e il responsabile della modifica stessa.

Come è possibile vedere dal grafico 1 l'andamento dei progetti risulta stagionale all'interno dei FY con picco a dicembre che va via via a scendere con la conclusione dei vari progetti fino a maggio.

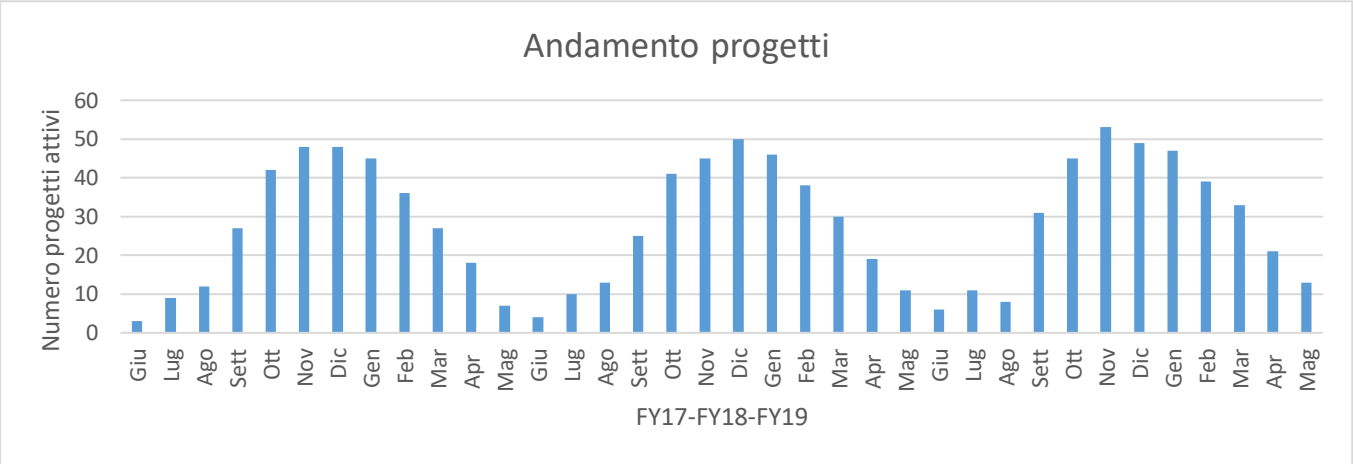


Grafico 4 Andamento progetti

Inoltre, i profitti risultano crescente in un orizzonte di 3 anni da un'analisi effettuata sul numero dei progetti con i rispettivi margini, come mostrato nel Grafico 2.

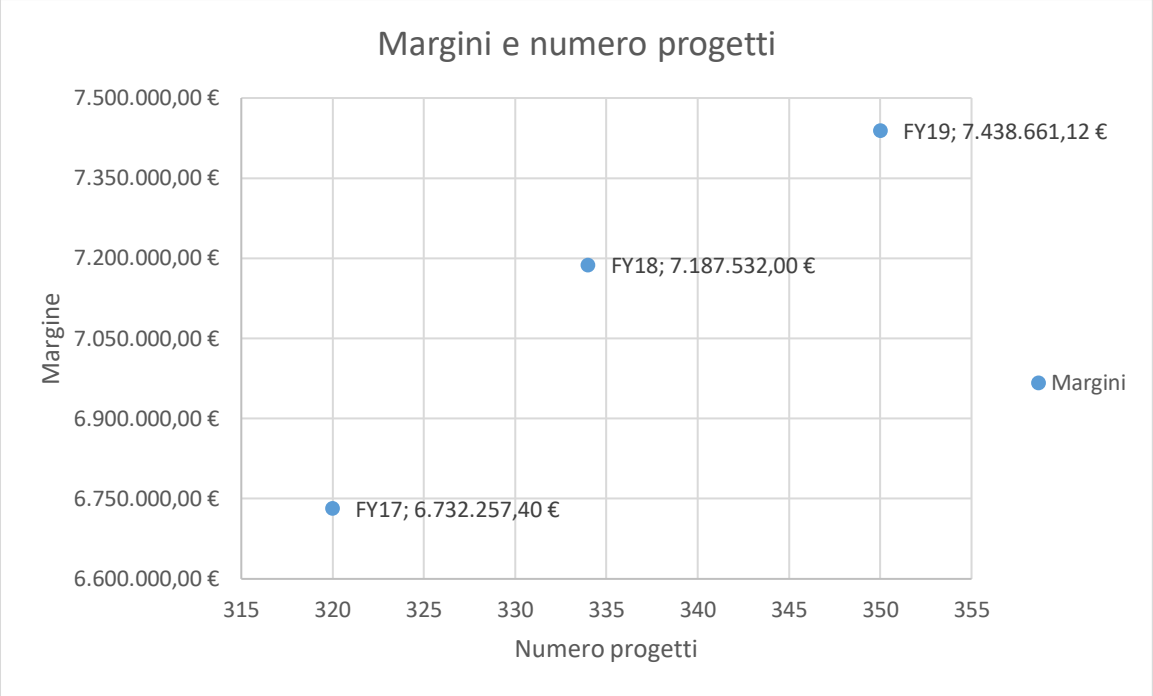


Grafico 5 Margini e numero progetti

- ORGANIZZAZIONE DEL LAVORO

L'organizzazione del lavoro è inefficiente, come dimostrato da:

- Ore di lavoro straordinario nei periodi di picco
- Alto turnover delle risorse
- Disallinemento della forza lavoro nelle varie sedi operative.

1) *Analisi Straordinari*

Per indagare sugli straordinari, è stato analizzato l'andamento delle ore ordinarie e straordinarie, suddivise in quindicine(di giorni), lavorate da quattro risorse nello scorso Fiscal Year.

Le risorse sono state scelte casualmente da un campione di 33 elementi e sono rispettivamente tre analyst e un senior che rappresentano dunque le prime la parte operativa del lavoro e l'altra la parte di review.

Come si può notare dai grafici 3, 4, 5, 6 i periodi con straordinari sono compresi tra novembre e maggio. Le ore di straordinario dichiarate dalle risorse raggiungono picchi di 40 ore per quindicina.

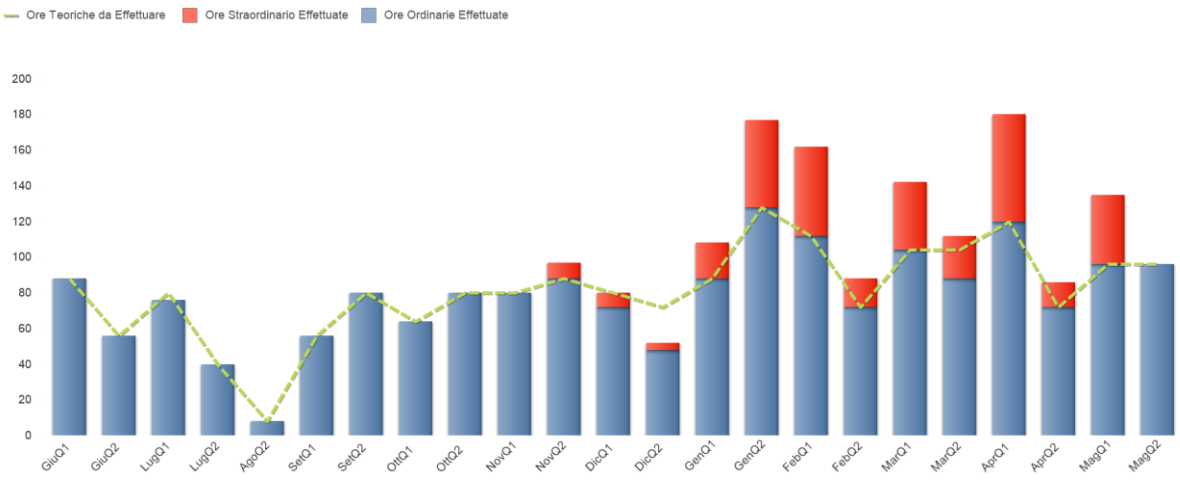


Grafico 6 Ore lavorate da Analyst A

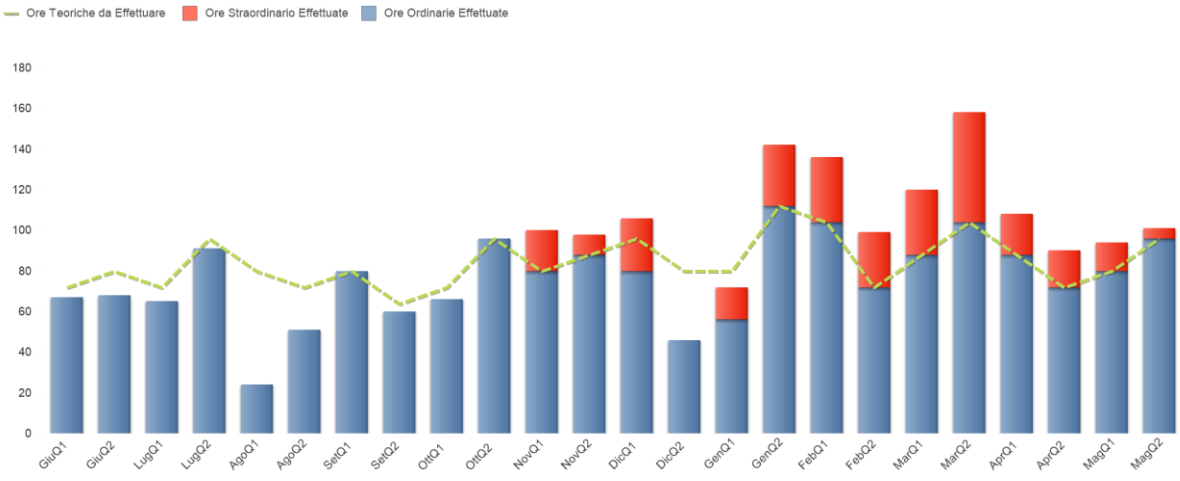


Grafico 7 Ore lavorate da Analyst B

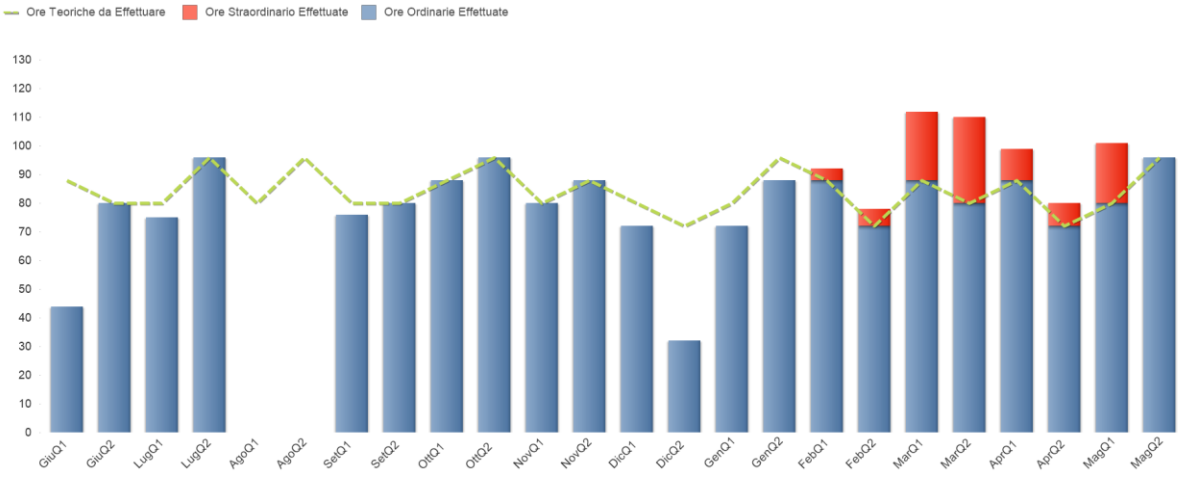


Grafico 8 Ore lavorate da Analyst C

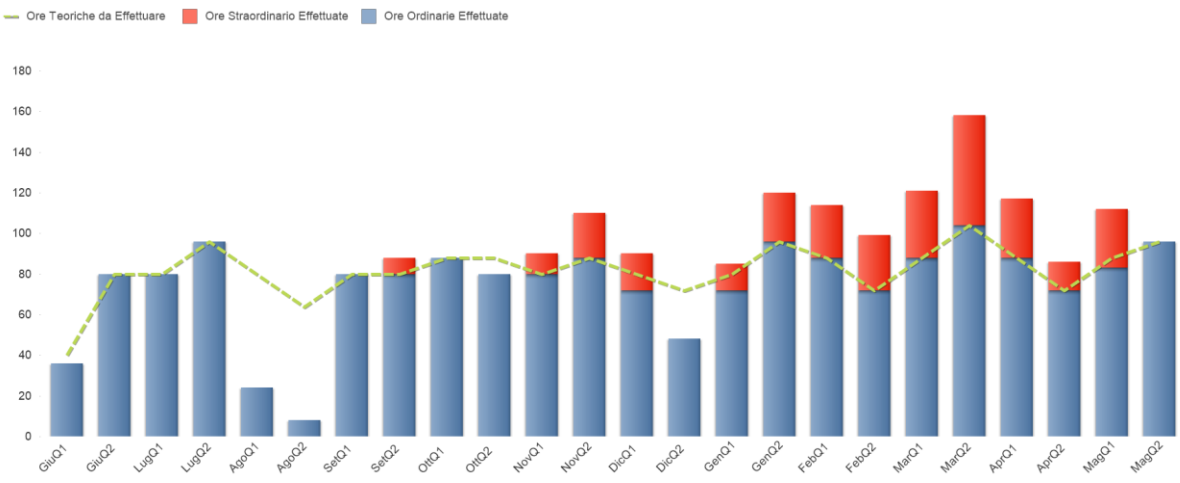


Grafico 9 Ore lavorate da Senior X

Gli straordinari si effettuano per riuscire a emettere giudizi sull'efficacia dei controlli entro la Data di Opinion e riuscire a completare la formalizzazione entro massimo 40 giorni da essa.

Poiché le date di consegna dei lavori si concentrano negli stessi periodi, le risorse si ritrovano a dover gestire un elevato numero di progetti contemporaneamente. Come riportato nel grafico 7, una singola risorsa può arrivare a dover lavorare su 9 progetti contemporaneamente.

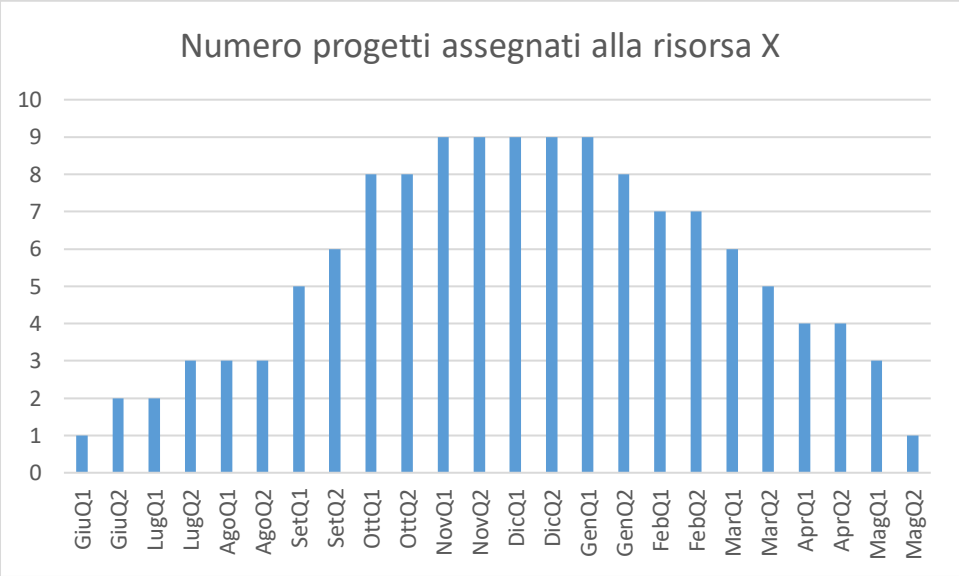


Grafico 10 Numero progetti gestiti dalla risorsa X

L'accumulo di molteplici progetti nello stesso periodo è dovuto a:

- Chiusura dei bilanci al 31 dicembre per la maggior parte delle società
- Ritardi nella recezione di evidenze da parte del cliente che portano allo slittamento delle attività di formalizzazione.
- Impossibilità di anticipare alcuni test sui controlli interni per la necessità di avere dati completi che coprono tutto il Fiscal Year. Esempi sono la lista dei dimessi per testare il corretto accesso ai sistemi informativi, ovvero la corretta cancellazione delle utenze.
- Ripetizione delle attività di test per correggere gli errori commessi emersi dalle review, dovuti all'inesperienza delle risorse.

Il costo dello straordinario varia a seconda del periodo:

- Straordinario= ordinario + 25% per le ore settimanali
- Straordinario= ordinario + 40% per le ore lavorate nei sabati e nelle domeniche

Nel 2019 il costo dello straordinario ha generato un'inefficienza in termini di aumento di costi del circa 14%.

Numero progetti_FY19	Ore straordinario	Straordinari	Costi	Incidenza straordinari
350	1620	374.598,40 €	2601098,88 €	**14%**

Gli elevati straordinari potrebbero essere la conseguenza di una mancanza di risorse, in quanto quelle presenti non sono sufficienti a sostenere il carico di lavoro. Si sono calcolate, allora, le ore di straordinario e i costi straordinari associati a ciascuna tipologia di risorsa nel FY 2019.

I costi straordinari sono stati ricavati utilizzando come incremento del rate orario ordinario 36%.

L'incremento del rate di orario straordinario è stato ricavato dal sondaggio sottoposto ai dipendenti. La domanda mirava a indagare sulla tipologia delle ore di straordinario effettuate, vedi figura 2.

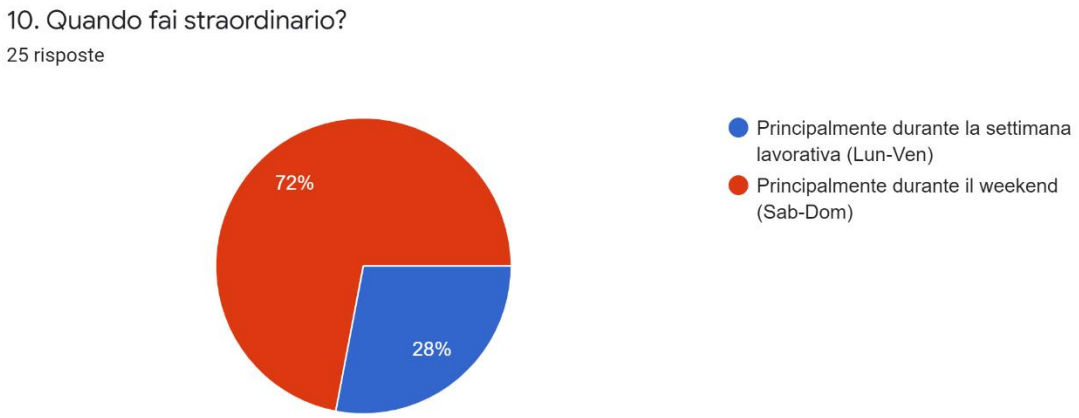


Figure 4.2 Questionario

Poiché il 72% dei rispondenti ha confermato di lavorare prevalentemente nel weekend e solo il 18% effettua lavoro straordinario durante la settimana, si è ricavato l'incremento x come:

$$0{,}4n + 0{,}25(1 - n) = x$$

dove 0,4 e 0,25 sono i sopra citati incrementi di rate

n=0,72*25=18 (numero risorse che lavorano nel weekend).

Dai risultati mostrati in figura #, emerge che non è conveniente assumere più risorse per ridurre gli straordinari perché essi non sono poi così elevati (circa 360.000€).

Vi è da considerare che una risorsa assunta rappresenta un costo fisso per l'azienda che dovrà essere pagato di mese in mese, mentre le ore straordinarie possono essere erogate o meno per cui rappresenta un costo variabile che non sempre viene pagato.Sono stati calcolati per ogni risorsa, in base alle ore di straordinario svolte, il numero aggiuntivo di figure necessarie come:

$$\Delta impiegati = \frac{Costo\ straordinario}{Ral+Tasse+bonus}$$

Esso risulta sempre non significativo ed al massimo una risorsa in più.

Ruolo	Ore straord	Rate orario	Costo straordinario	RAL (K€)	BONUS (K€)	Tasse 35%	Tasse + bonus	Δimpiegati
Analyst	433	70	41.221,60 €	25		33,75	33,75	1,15
Analyst 2	266	85	30.749,60 €	28		37,8	37,8	0,76
Consultant	175	160	38.080,00 €	30	1	40,5	41,5	0,85
Senior Consultant	264	190	68.217,60 €	37,5	2	50,625	52,625	1,21
Manager	199	240	64.953,60 €	45	10	60,75	70,75	0,86
Senior Manager	205	300	83.640,00 €	50	14	67,5	81,5	0,96
Partner	78	450	47.736,00 €	70	30	94,5	124,5	0,35
Totale	**1620**		374.598,40 €					

Tuttavia i calcoli sono molto approssimativi perché le risorse dichiarano davvero poche ore di straordinario rispetto a quanto effettuato. Il manager deve infatti approvare il numero di ore straordinarie a seconda che ci sia o meno budget disponibile da erodere per poterle remunerare. Dal questionario è emerso che la quasi totalità delle risorse svolge spesso ore di straordinario, come mostrato in figura 3.

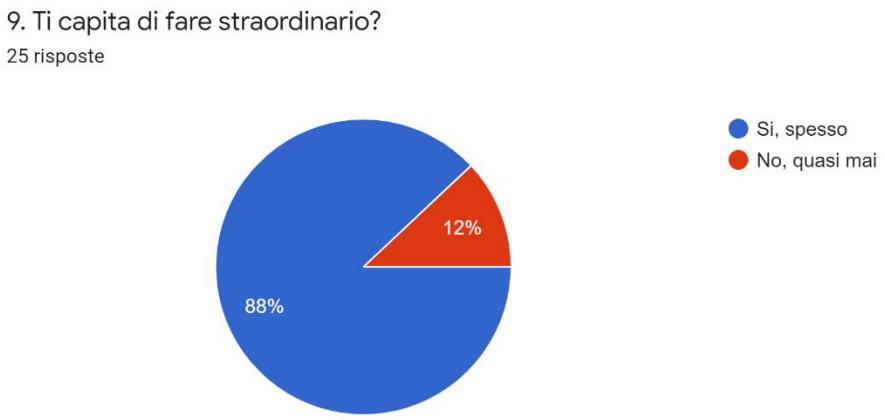


Figure 4.3 Questionario

I carichi di lavoro incidono anche sulla qualità del report emesso. Spesso a ridosso delle scadenze le formalizzazioni risultano poco dettagliate o approssimative per la mancanza di tempo, per cui è necessario effettuare più review dello stesso lavoro per arrivare a una qualità di report accettabile.

2) *Turnover risorse*

Al fine di indagare sul turnover delle risorse sono stati confrontati gli Scheduling del personale degli ultimi 3 fiscal year e con delle VLOOKUP si sono ricavati il numero di nuovi assunti e dimessi in ciascuno di essi.

Il tasso di Turnover delle risorse è stato calcolato come:

$$Turnover = \frac{Nuovi\ Assunti + Dimessi}{Impiegati}$$

Il turnover del numero totale di risorse oscilla tra 0,62 e 0,74, per cui risulta elevato. L'andamento delle risorse complessivo è riportato nel grafico 8, a cui seguono le divisioni per ruolo nei grafici 9, 10, 11.

FY	Impiegati	Dimessi	Nuovi Assunt	TURNOVEI
FY17	27	11	9	0,74
FY18	28	7	12	0,68
FY19	34	9	12	0,62

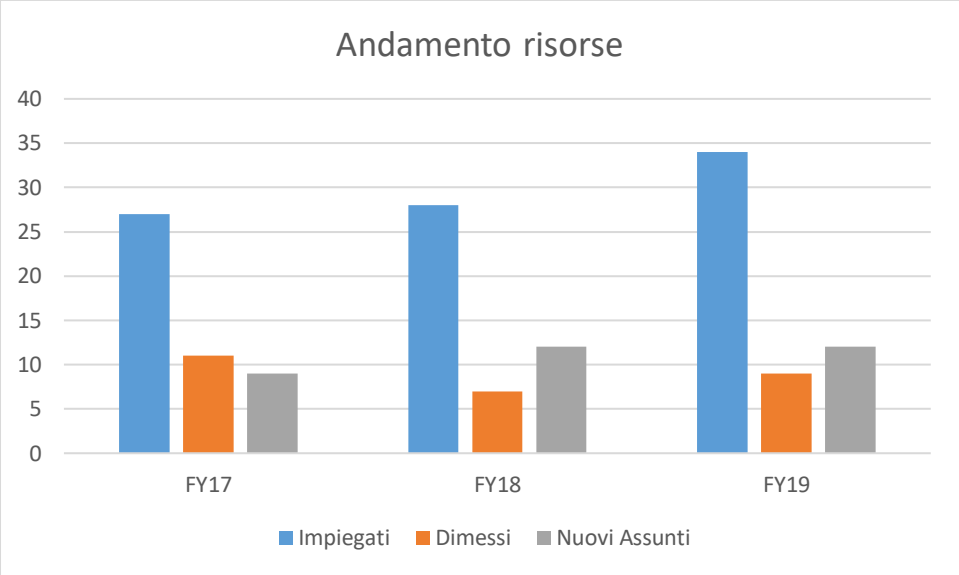


Grafico 11 Andamento risorse

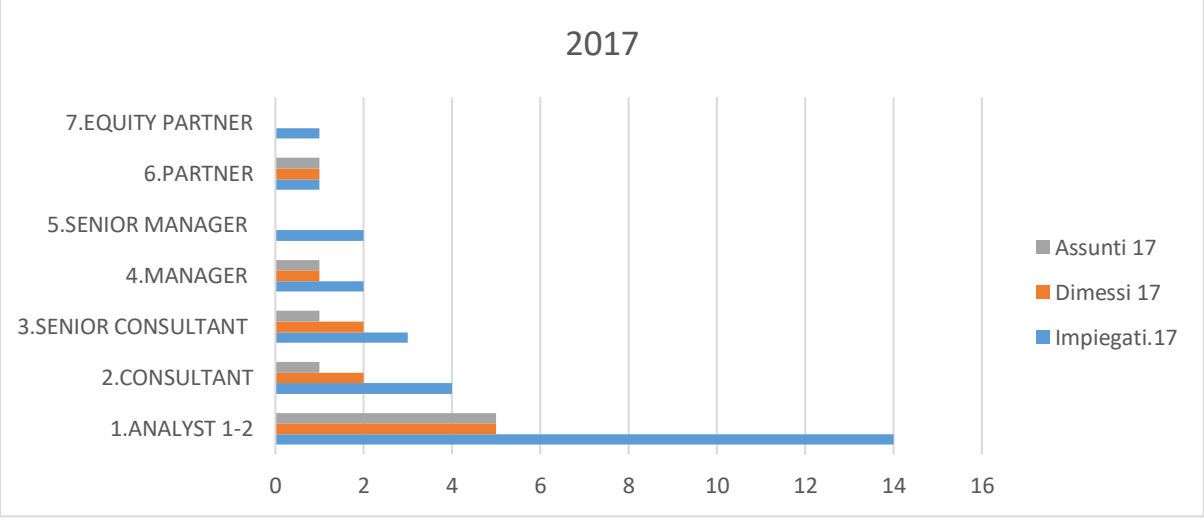


Grafico 12 Andamento risorse FY17

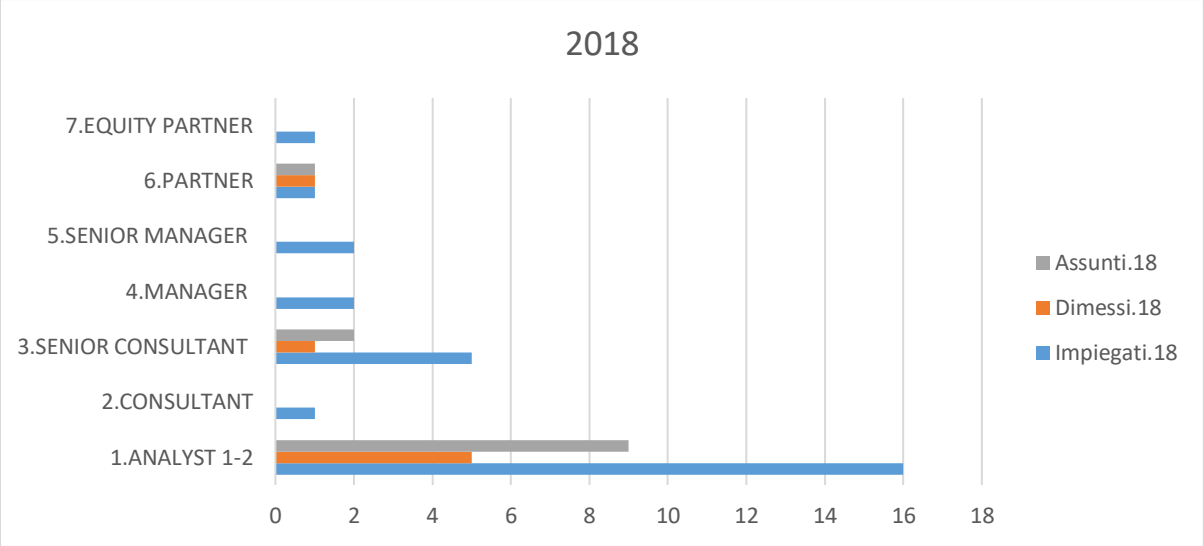


Grafico 13 Andamento risorse FY18

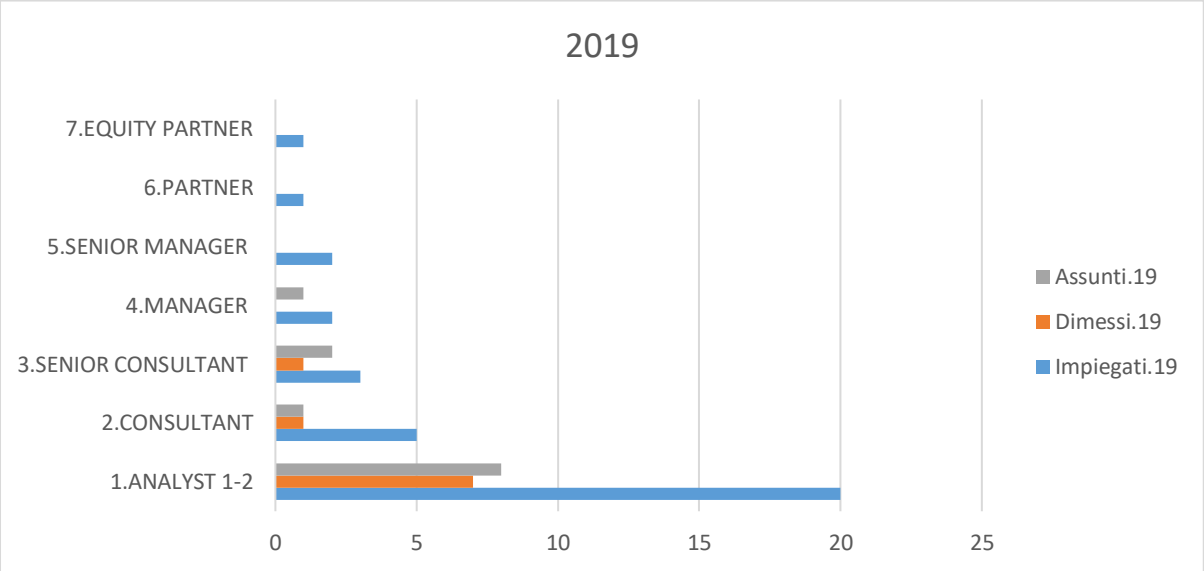


Grafico 14 Andamento risorse FY19

Dal confronto tra i 3 anni si nota che il numero di risorse è crescente, coerentemente con l'andamento della domanda e che la rotazione maggiore di risorse è tra gli Analyst, come mostrato nel grafico 12, con tassi di turnover che raggiungono quasi il 90%.

FY	ANALYST	ANALYST DIMESSI	ANALYST ASSUNTI	Turnover
FY17	14	5	5	71,4%
FY18	16	5	9	87,5%
FY19	20	7	8	75,0%

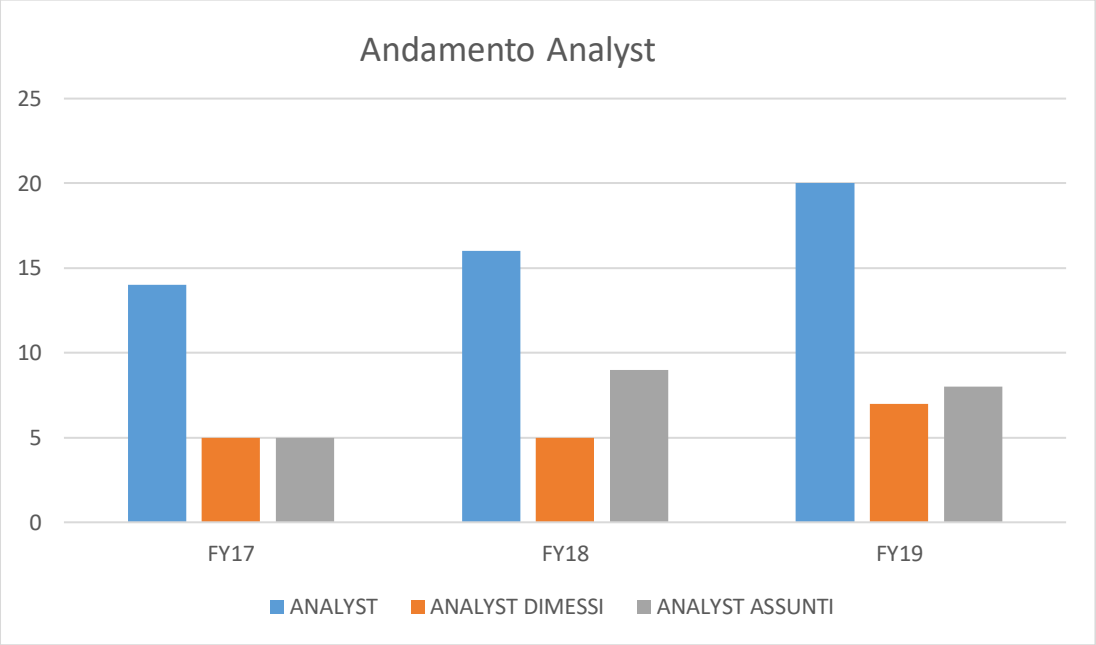


Grafico 15 Andamento Analyst

L'alto turnover incide anche sulla qualità del lavoro perché:

- il continuo ricambio di risorse determina la prevalenza di personale inesperto (poco skillato)
- la bassa permanenza in azienda non permette di creare economie di specializzazione.

Dal questionario emerge che solo il 16% dei rispondenti è presente in azienda da più di due anni, vedi figura 4.

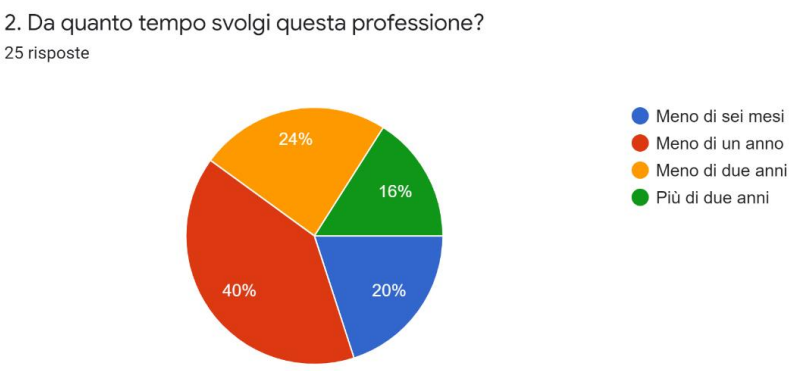


Figure 7.4 Questionario

Riassumendo lo scenario attuale è contrassegnato da una domanda crescente, con problemi di carico di lavoro che insieme ad un alto turnover delle risorse incide sulla qualità del lavoro finale.

4.2 Proposta di applicazione dell'RPA al processo

Per la valutazione di una proposta di applicazione dell'RPA al processo si sono formulati dei criteri qualitativi per stimare la sua complessità.

Tra le operazioni più critiche vi sono l'analisi dei dati in input, poiché essi possono essere sia strutturati che non strutturati. La macchina deve essere in grado di riuscire a leggere i dati in diversi formati quali immagini, pdf, email, excel per cui la complessità risulta elevata in quanto è necessario applicare Natural Language Processive e Cognitive Intelligence. In aggiunta, il numero di applicativi da gestire è elevato in quanto i clienti hanno spesso applicativi non standard ma customizzati per cui non è banale per la macchina capire dove reperire i dati di interesse.

Tuttavia, il numero di database e di sistemi operativi diversi da gestire non è elevato in quanto il livello di customizzazione è ridotto.

Il punto di forza che permette l'automazione del processo è costituito dal ripetersi delle procedure di analisi tra i diversi applicativi o tra i diversi DB e OS. Infatti, il numero di controlli diversi non è elevato, ma sono comuni per la maggior parte dei sistemi.

Il numero di operazioni è inteso come numero di step che la macchina deve effettuare, dalla raccolta iniziale dei dati da prelevare all'effettiva analisi degli stessi seguendo la procedura.

Ad ogni criterio è stata assegnata una valutazione 1-2-3 a seconda che sia ritenuto poco complesso, mediamente complesso o molto complesso.

Si riporta di seguito il dettaglio dei criteri in tabella 1:

Table 4 Criteri Complessità

Criteri / grado complessità	Numero di operazioni	Tipi di applicativi diversi	Tipi di database diversi	Tipi di sistemi operativi diversi	Numero di controlli diversi tra applicativi	Numero di controlli diversi tra database	Numero di controlli diversi tra sistemi informatvi	Tipologia di dati in input
Bassa Complessità	<25	1--15	1--4	1--4	<5	<5	<5	Dato di input digitale, strutturato e standardizzato
Media Complessità	25-50	15--30	5--9	5--9	5--15	5--15	5--15	Dato di input digitale strutturato e non standardizzato
Alta Complessità	>50	>30	>9	>9	>15	>15	>15	Dato di input digitale, non strutturato e non standardizzato
Valore	**>60**	**>40**	**7**	**4**	**10**	**2**	**2**	**Dato di input digitale, non strutturato e non standardizzato**
Grado di complessità	**3**	**3**	**2**	**1**	**2**	**1**	**1**	**3**

La stima risultante della complessità del processo è 2, ovvero media complessità, per cui ha una predisposizione all'automazione poichè qualsiasi **task basato su regole di business strutturate e ripetibili poco complesse** si qualifica per l'automazione.

Nuovo processo

La fase 1 di acquisizione del cliente resta invariata, in quanto è importante stabilire l'engagement. Essa presuppone dunque l'incontro diretto tra partner e azienda da auditare.

La fase 2 che prevede il kick off tra manager senior e cliente, per la stessa ragione di cui sopra non è automatizzata. Gli incontri diretti in queste prime due fasi sono indispensabili per costruire un rapporto di reliance tra le parti e fidelizzare il cliente per le revisioni future.

La fase 3 di raccolta dati è parzialmente automatizzata. Prevede che il robot operi in modalità attended (assistito e attivato da un operatore umano) in cui l'analyst inserisce i dati di input, ovvero la richiesta documentale che ha personalmente sviluppato valutando l'understanding redatto dal manager e i rischi che ha assegnato ai controlli nel risk assessment. La macchina dovrà poi andare a prelevare i dati direttamente nell'ambiente IT del cliente, nel caso in cui sia stato concesso da esso un accesso in remoto con rete VPN (Virtual Private Network) utilizzando un tool di automazione altamente visuale che comprende un registratore di processo e un set di attività di automazione precostituite che possono essere utilizzate per l'estrazione dei dati nel caso di applicativi standard. Nel caso in cui la macchina non riuscisse a trovare in autonomia i dati necessari all'interno del sistema informativo dovrà inviare delle mail

in totale autonomia con le richieste dettagliate di estrazione ai referenti IT e dovrà sollecitare in caso di ritardi nella ricezione.

La fase 4 di analisi della documentazione ricevuta è completamente automatizzata. La macchina dovrà, tramite algoritmi di Natural Language Processing e Cognitive Intelligence essere in grado di catturare automaticamente ogni step del processo di formalizzazione e replicare ogni sorta di workflow, leggere le policy aziendali per estrarre le informazioni utili a capire il design del controllo per poi implementarlo nel test dell'operating effectiveness. Nella valutazione dell'OE, la macchina segue una procedura standard che descrive per ogni controllo come effettuare il test associato, adoperando attraverso match dei dati fino a proporre un giudizio sul controllo (effective o deficiency) e riportando tutte le analisi su un report. Il robot sfrutta architetture di AI che usano intelligenza cognitiva per vedere, capire ed agire su contenuti anche non strutturati utilizzando modelli di machine learning, per cui il robot è in grado imparare dall'esperienza non soltanto da regole e procedure predefinite.

La fase 5 prevede una prima review da parte dell'analyst che valuta i report sviluppati dalla macchina e decide se far effettuare ad essa eventuali rework o svolgerli manualmente. La review finale è effettuata da senior e manager che decidono sull'approvazione del lavoro. La durata della review rispetto al processo non automatizzato è ridotta in quanto si riduce il rischio di errore dovuto alla natura manuale delle attività. Si passa, infatti, da un'accuratezza dell'analisi del 90% a una del 97,3%[40].

In parallelo alla fase 3 e 4 è il lavoro dei robot controllers che effettuano i test sul funzionamento della macchina e degli RPA developers che sviluppano codice per la gestione di nuovi applicativi.

Sviluppo della macchina RPA

Lo sviluppo di un software RPA che svolga le attività sopra descritte è complesso in quanto non esistono ancora prodotti simili così avanzati sul mercato. La stima di costi e tempi di realizzazione è dunque approssimativa ma non certa.

40

Data l'incertezza dell'ambiente tecnologico, si sono ipotizzati due scenari:

- Automazione del 50% delle attività umane ripetitive
- Automazione spinta del 93% delle attività umane ripetitive.

Le percentuali di automazione sono state ricavate dagli studi effettuati dalle Big 4, in cui prevedono una sostituzione parziale e/o quasi totale delle attività ripetitive svolte dall'audit. La sostituzione è ad opera di software intelligenti in grado raccogliere dati, testarli e formalizzare i controlli sui sistemi informativi dei clienti auditati con prestazioni di lavoro che arrivano a rapporti di 1 minuto macchina per approssimativamente 15 minuti uomo.[41] L'automazione al 50% appare più realistica in quanto la macchina continua ad essere assistita dall'operatore umano con il ruolo di supporto per velocizzare le operazioni di matching dei dati nelle operazioni di operating effectiveness.

Per lo sviluppo della macchina RPA si è ipotizzato un co-development della società di consulenza con una società leader di innovazione di RPA e IA (come UiPath e BluePrism). Lo sviluppo interno non è infatti realisticamente realizzabile, in quanto, la società di consulenza non ha ancora ne le competenze ne gli strumenti necessari per lo sviluppo di una tecnologia così avanzata a costi ragionevoli. Per entrambi gli scenari si è ipotizzata comunque l'assunzione di personale developer esperto di RPA che collabori con la società esterna e impari da essa per proseguire le attività di sviluppo in modo autonomo dopo la fine del contratto. L'obiettivo è di istituire un Centro di Eccellenza CoE interno alla società di consulenza per creare un team di RPA specialist con abilità di analisi e individuazione di processi candidabili all'automazione, effettuare design e testing automi, delivery e gestione esercizi.

La remunerazione della società tecnologica avviene con una royalties% sul fatturato totale con la copertura dei costi vivi di sviluppo del personale e delle licenze software necessarie. Si è applicato il meccanismo di Innovation sharing, in cui la società di consulenza copre tutti i costi relativi alla ricerca e allo sviluppo della nuova tecnologia. La società tecnologica evita così meccanismi di hold up contrattuali a causa dell'investimento specifico in una tecnologia in parte custumizzata per la società di

[41] Automate this: The business leader's guide to robotic and intelligent automation, Deloitte

consulenza. D'altro canto però la società tecnologica si impegna a non diffondere il know how generato dalla collaborazione nello sviluppo dell'RPA e di riservare diritti di esclusività per il periodo contrattuale concordato.

Scenario iniziale senza RPA

La situazione attuale non prevede automazione. Negli allegati 1, 2, 3 si riportano i calcoli relativi alla valutazione di tre progetti di:

- Clienti piccoli (Budget< 20 K€)
- Clienti medi (20K€<= Budget < 90 K€)
- Clienti grandi (Budget>=90 K€)

Le attività svolte per tutti i clienti sono:

1) Acquisizione cliente, Understanding of IT Environment e kick off effettuati in trasferta da partner, manager e senior consultant
2) General IT controls su applicativi, database e OS

Si aggiungono per i clienti medi e grandi:

3) Controlli Automatici
4) Analisi IPE e IUC

I clienti grandi hanno ancora:

5) Analisi interfacce
6) JET
7) Analisi Datawarehouse

Questi tre progetti sono stati presi da esempio per calcolare in media i ritorni annuali considerando la seguente composizione dei progetti durante il FY19:

PROGETTI FY19		
Tipologia Progetto	**Numero Progetti**	**Composizione Team Audit**
Grande	20	1 partner, 1 manager, 1 senior consultant, 1 consultant, 1 analyst II, 3 analyst I

Medio	86	1 partner, 1 manager, 1 senior consultant, 1 consultant, 1 analyst II, 1 analyst I
Piccolo	244	1 partner, 1 manager, 1 senior consultant, 1 analyst1.
TOTALE PROGETTI	350	

Il budget del progetto si calcola andando a moltiplicare le ore lavorate da ciascun team member per il rate orario, ovvero il prezzo dell'ora venduta al cliente che è molto maggiorata rispetto al reale costo orario ricavato dallo stipendio annuale, come si può evincere dalla tabella riportata di seguito:

Ruolo	Rate orario (€/h)	Costo orario (€/h)
Analyst 1	70,00	16,67
Analyst 2	85,00	18,68
Consultant	160,00	20,01
Senior Consultant	190,00	25,01
Manager	240,00	30,01
Partner	450,00	46,69

I costi delle trasferte sono stati calcolati come mostrato nell'allegato 4, andando ad individuare la collocazione geografica dei 350 clienti, classificandoli per aree Nord, Centro, Sud, Lombardia, Milano.

Il costo si compone della somma:

- costo viaggio A/R (se fuori da Milano) pari a 50€ Lombardia, 150€ Nord, 180€ Centro, 220€ Sud
- costo alloggio pari a 120€/notte
- diaria, retribuzione aggiuntiva data alla risorsa per viaggi fuori da Milano della durata di almeno 8h pari a 56€. Per la Lombardia è stata considerata la mezza-diaria pari a 25€.

Il costo degli straordinari è quello risultante del FY 2019, di cui si era mostrato il calcolo in precedenza.

Dall'analisi risulta che il ricavo totale, facendo la semplificazione che i budget dei progetti delle tre categorie (grande, medio, piccolo) siano costanti e/o compensativi, è di circa 10 Milioni €, con un margine che comprende costi operativi, trasferte e straordinari pari al 74%.

I costi totali non corrispondono esattamente alla somma degli stipendi dei singoli dipendenti ma risultano maggiorati di circa 400.000€. Tale cifra è dovuta al fatto che, nella maggior parte dei casi, altre risorse non appartenenti all'ufficio in questione,ma appartenenti comunque alla società di consulenza, svolgono attività di revisione per conto dell'ufficio preso in esame.

(Per esempio una risorsa appartenente a GUASIM Torino revisiona un cliente acquisito da GUASIM Milano ma non fa parte dell'organigramma interno di GUASIM Milano. Tale risorsa viene "presa in prestito" da un altro ufficio appartenente comunque alla società di consulenza in questione per lo svolgimento della revisione a causa di una temporanea mancanza di risorse. La risorsa in questo caso fattura per GUASIM Milano, ragion per cui GUASIM Milano paga altri stipendi di personale esterno all'ufficio in questione e presenta maggiori costi del personale rispetto a quelli presente nella sua sede.)

Size	**Piccolo**	**Medio**	**Grande**
Numero_progetti	244	86	20
Ricavo singolo progetto	**10.200,00 €**	**55.560,00 €**	**138.640,00 €**
Costi personale singolo progetto	1.727,52 €	9.321,94 €	27.043,35 €
Margine singolo progetto	8.472,48 €	46.238,06 €	111.596,65 €
Margine totale progetti per size	2.067.285,18 €	3.976.473,44 €	2.231.932,91 €
Margine TOTALE		**8.275.691,52 €**	
Costo trasferte		462.432,00 €	
Costo straordinari		374.598,40 €	
Margine finale		**7.438.661,12 €**	

Scenario Automazione al 50%

Nello scenario di automazione parziale si vuole sviluppare una macchina RPA in grado di raccogliere in automatico i dati dagli applicativi, database e sistemi operativi dei vari clienti adoperando in modo simile all'ACTT tool descritto nel Capitolo 3 e poi svolgere in modo automatico i test sull'Operating Effectiveness dei controlli. La macchina è a

supporto dell'Analyst, velocizzando le sue attività, ma non sostituendolo. Il compito dell'Analyst è ancora quello di intervistare il cliente telefonicamente o direttamente con trasferte per indagare sui controlli effettuati e capirne il design. Lo strumento fornito all'Analyst sarebbe una macchina in grado di matchare i dati e le informazioni utili all'esecuzione del controllo per verificare l'operatività dello stesso. Il giudizio finale sull'efficacia o meno dei controlli è ancora umano.

Si sono analizzati di nuovo i tre progetti precedenti, aggiungendo l'RPA come mostrato negli allegati 4, 5, 6. Applicando il rapporto 1 minuto macchina - 2 minuti uomo, si sono dimezzate le ore di lavoro nella raccolta dati, nei General IT Controls, nei Controlli Automatici, IPE e IUC, Analisi interfacce e Datawarehouse e JET in quanto si suppone che la macchina riesca ad effettuare il test sull'Operating Effectiveness che rappresenta circa il 50% del controllo da effettuare. Anche la review finale da parte del senior consultant, manager e partner si dimezza poiché automatizzando parte del processo si riducono gli errori umani.

In questo scenario sono ancora necessarie le trasferte per cui si è considerato un importo di valore invariato rispetto allo scenario iniziale. Gli straordinari si annullano perché la macchina essendo più veloce riesce ad assorbire i carichi di lavoro.

Il costo dell'automazione è pagato in termini di royalties% sui ricavi totali, stimata in base a benchmark con prodotti simili realizzati al 6%. È stato aggiunto il costo di 4 developers con una RAL=50.625€ annuale.

Size	**Piccolo**	**Medio**	**Grande**
Numero_progetti	244	86	20
Ricavo singolo progetto	**10.200,00 €**	**55.560,00 €**	**138.640,00 €**
Costi RPA (fee=6%)	612,00 €	3.333,60 €	8.318,40 €
Costi personale singolo progetto	1.018,84 €	4.957,78 €	14.136,98 €
Margine singolo progetto	8.569,16 €	47.268,62 €	116.184,62 €
Margine totale progetti per size	2.090.875,90 €	4.065.101,18 €	2.323.692,38 €
Margine TOTALE		**8.479.669,46 €**	
Costo developers (4)		202.500,00 €	
Costo trasferte		462.432,00 €	
Costo straordinari		0,00 €	
Margine finale		**7.814.737,46 €**	

Dall'analisi risulta che il ricavo totale, di nuovo facendo la semplificazione che i budget dei progetti delle tre categorie (grande, medio, piccolo) siano costanti e/o

compensativi, è di circa 10 Milioni € (distorsione dal budget reale del 9%), poiché si suppone che il prezzo offerto al cliente resti invariato. Il margine che comprende costo automazione, costi operativi, trasferte e straordinari è pari al 78%.

Costo sviluppo macchina

Per la stima dei costi di sviluppo della macchina RPA si è utilizzato il "COCOMO II Model", la cui spiegazione si riporta in dettaglio nell'Appendix A.

Per lo sviluppo della macchina RPA è stato considerato un numero di SKLOC pari a 250 in base a stime derivate da progetti simili e considerando che parte di codice relativo alla raccolta dati su applicativi, DB, OS standard sono già stati sviluppati dalla società tecnologica. Inoltre, si è considerato che gli internal developers della società di consulenza continuino il processo di sviluppo per adattare il codice anche ai clienti che hanno sistemi più customizzati.

Il dettaglio sul calcolo dell'esponente B dell'effort e dell'EAF è riportato nell'allegato 7.

L'Effort richiesto per lo sviluppo della macchina, come si può vedere nella tabella sottostante è pari a 651 person*month, per un tempo di sviluppo pari a 35 mesi con 18 sviluppatori.

PARAMETRI		
A	Costante	2,94
B	1,01+0,01*SUM(SF)	1,1607
SKLOC	Costante	250
EAF	PROD(CF)	0,36
SCENARIO RPA 50%		
EFFORT (Person*month)	A*(KLOC)^B*EAF	651,3752156
DEVELOPMENT TIME (Month)	[3*EFFORT^(0,33+0,2*(B-1,01)]*SCED%/100	35
AVARAGE STAFF SIZE (Person)	EFFORT/(DEVELOPMENT TIME)	18
PRODUCTIVITY (KLOC/Person*month)	KLOC/EFFORT	38%

Considerando una giornata lavorativa pari a 8h (ore lavorate in un mese 8h/day*5day/week*4week/month=160h) con uno stipendio orario di 17,95€/h si sono calcolati i costi legati alle risorse necessarie allo sviluppo dell'RPA.

Sono stati stimati costi legati alle componenti IT Hardware e software pari a circa 30K€ (legato al costo di utilizzo di licenze necessarie per lo sviluppo della tecnologia) e un

contingency budget pari al 4% dei Total Capex. Il costo totale dell'investimento iniziale risultante è di 1,9 milioni di €.

Investimento Iniziale	
Costo personale programmatore	**1.809.360,00 €**
IT hardware e software	**29.750,00 €**
Contingency	**80.000,00 €**
Total capex	**1.919.110,00 €**

Scenario Automazione al 93%

Nello scenario di automazione quasi totale si vuole sviluppare una macchina RPA in grado di raccogliere in automatico i dati degli applicativi, database e sistemi operativi direttamente dai sistemi informativi aziendali attraverso accesso diretto mediante VPN, mediante l'utilizzo di tool automatici per la raccolta dati oppure tramite mail inviate automaticamente al cliente auditato. La macchina sarà in grado di svolgere in modalità unattended sia il test sul design, andando ad analizzare i documenti in cui sono descritte le policy aziendali o le prassi aziendali e confrontandoli con le procedure degli anni passati in caso di clienti storici, sia il test sull'operating effectiveness, fornendo l'esito sui controlli.

Si sono analizzati i tre progetti precedenti, aggiungendo l'RPA come mostrato negli allegati 8, 9, 10. Applicando il rapporto 1 minuto macchina - 15 minuti uomo, si sono ridotte maggiormente le ore di lavoro uomo nella raccolta dati, nei General IT Controls, nei Controlli Automatici, IPE e IUC, Analisi interfacce e Datawarehouse e JET. Anche la review finale da parte del senior consultant, manager e partner è stata ridotta proporzionalmente.

Un'automazione così spinta comporta una riorganizzazione quasi totale del lavoro, determinando nuovi task, eliminandone altri e sostituendo il personale con risorse più "skillate" tecnologicamente. Infatti, non sono richieste solo competenze specialistiche specifiche della RPA: sono essenziali anche la gestione del progetto, dei processi e le competenze di gestione del cambiamento.

Le ore umane delle risorse operative, rimanenti nello svolgimento del progetto sono in qualifica di robot controller, ovvero per assegnare i lavori ai robot e per monitorare le loro attività.

In questo scenario le trasferte necessarie sono solo quelle della fase iniziale, ovvero di acquisizione e kick off con il cliente per cui si è considerato un importo di valore inferiore rispetto allo scenario iniziale, come mostrato nell'allegato 12. Gli straordinari, di nuovo sono nulli perché la macchina essendo più veloce riesce ad assorbire i carichi di lavoro.

Il costo dell'automazione è pagato in termini di royalties% sui ricavi totali, stimata in base a benchmark con prodotti altamente tecnologici simili realizzati al 10,5%. È stato aggiunto il costo di 8 developers con una RAL=50.625€ annuale, in quanto il processo necessita di continua maintenance e aggiornamenti.

Size	**Piccolo**	**Medio**	**Grande**
Numero_progetti	244	86	20
Ricavo singolo progetto	**10.200,00 €**	**55.560,00 €**	**138.640,00 €**
Costi RPA (fee=10,5%)	1.071,00 €	5.833,80 €	14.557,20 €
Costi personale singolo progetto	404,64 €	1.175,51 €	2.951,46 €
Margine singolo progetto	8.724,36 €	48.550,69 €	121.131,34 €
Margine totale progetti per size	2.128.742,80 €	4.175.359,01 €	2.422.626,85 €
Margine TOTALE		**8.726.728,66 €**	
Costo developers (4)		405.000,00 €	
Costo trasferte		116.382,00 €	
Costo straordinari		0,00 €	
Margine finale		**8.205.346,66 €**	

Mantenendo i ricavi costanti, attuando le stesse semplificazioni degli scenari precedenti, si ottiene un margine che comprende costo automazione, costi operativi, trasferte e straordinari è pari all'82%.

Costo sviluppo macchina

Per lo sviluppo della macchina RPA è stato considerato un numero di SKLOC pari a 450 in base a stime derivate da progetti simili, tenendo conto della maggiore complessità di realizzazione rispetto allo scenario 0,5 e mantenendo le stesse assunzioni fatte in precedenza.

Il dettaglio sul calcolo dell'esponente B dell'effort e dell'EAF è riportato nell'allegato 11.

L'Effort richiesto per lo sviluppo della macchina, come si può vedere nella tabella sottostante è pari a 1104 person*month, per un tempo di sviluppo pari a 51 mesi con 22 sviluppatori.

PARAMETRI		
A	Costante	0
B	1,01+0,01*SUM(SF)	1,11
SKLOC	Costante	450
EAF	PROD(CF)	0,43
SCENARIO RPA 93%		
EFFORT (Person*month)	A*(KLOC)^B*EAF	1103,775655
DEVELOPMENT TIME (Month)	[3*EFFORT^(0,33+0,2*(B-1,01)]*SCED%/100	51
AVARAGE STAFF SIZE (Person)	EFFORT/(DEVELOPMENT TIME)	22
PRODUCTIVITY (KLOC/Person*month)	KLOC/EFFORT	41%

Il costo delle risorse è stato stimato utilizzando lo stesso rate orario del caso precedente.

Sono stati stimati costi legati alle componenti IT Hardware e software pari a circa 40K€ (legato al costo di utilizzo di licenze necessarie per lo sviluppo della tecnologia) e un contingency budget pari al 3% dei Total Capex. Il costo totale dell'investimento iniziale risultante è di 3,36 milioni di €.

Investimento Iniziale	
Costo personale programmatore	**3.222.384,00 €**
IT hardware e software	**40.800,00 €**
Contingency	**100.000,00 €**
Total capex	**3.363.184,00 €**

CONFRONTO SCENARI

	SITUAZIONE ATTUALE		
	Senza RPA	**RPA(0,5)**	**RPA(0,067)**
Ricavi Totali	10.039.760,00 €	10.039.760,00 €	10.039.760,00 €
Royalty annuali	- €	602.385,60 €	1.054.174,80 €
Costi totali personale	1.764.068,48 €	957.704,94 €	258.856,54 €
Straordinari	374.598,40 €	- €	- €
Trasferte	462.432,00 €	462.432,00 €	116.382,00 €
Costo internal developers	- €	202.500,00 €	405.000,00 €
IT components and mantainence		22.500,00 €	50.000,00 €
Margini Totali	7.438.661,12 €	7.792.237,46 €	8.155.346,66 €
Calcolo ritorni			
Gross Savings		**978.461,94 €**	**1.820.860,34 €**
Royalty annuali		602.385,60 €	922.595,00 €
IT components and maintenance		22.500,00 €	50.000,00 €
Net Saving		**353.576,34 €**	**848.265,34 €**
Total Capex		**1.919.110,00 €**	**3.363.184,00 €**
Payback		*Tra 8-9 anni*	*Tra 5-6 anni*
Orizzonte Temporale 5 anni			
ROI		*-30%*	*-4%*
VAN(5 anni)		*- 578.777,50 €*	*- 147.590,98 €*
Orizzonte Temporale 10 anni			
ROI		*13%*	*55%*
VAN(10 anni)		*253.463,53 €*	*1.849.039,29 €*

Da un'analisi costi/benefici effettuata sui 3 scenari presi in considerazione, emerge che una maggiore automazione si traduce in un maggior margine totale considerando il fatturato totale uguale nei 3 casi, con 350 progetti totali.

Infatti, il margine è aumentato del 4,75% nel caso di un'automazione al 50%, a fronte di un investimento iniziale pari a 1.919.110,00€. In questo scenario è avvenuta una sostituzione di lavoro con capitale che a parità di mansioni effettuate, risulta conveniente dal punto di vista economico. Il costo del lavoro si è ridotto del 45,75%, nonostante il parziale riassorbimento delle risorse (4 internal developers assunti ma circa 11 dipendenti dimessi per un totale di 7 risorse "perse"). Inoltre, vi è la totale eliminazione degli straordinari (inefficienza del processo) e il costo delle trasferte rimane inalterato, in quanto, a questo livello di automazione, risultano ancora totalmente necessarie. Infatti, anche se il numero di impiegati complessivi diminuisce, il numero di progetti assegnati ad ogni singola risorsa aumenta, per cui ogni risorsa compie più trasferte rispetto al caso in assenza di automazione. La composizione del costo totale risulta essere pari al 73% lavoro e 27% capitale contro il 100% del caso

iniziale. La riduzione del lavoro comporta un *Gross Savings= 978.461,94€* che al netto dei costi legati all'automazione, quali le royalties pari al 6% del fatturato lordo e i componenti e alla maintenance IT, porta un *Net Savings= 353.576,34€.*

Nel caso di automazione del 93%, il margine totale è aumentato del 9,63%. A fronte di un investimento iniziale 3.363.184 € (75% superiore a quello di RPA pari al 50%), il costo del lavoro si è ridotto del 70% rispetto al caso senza RPA (51,92%rispetto al caso con RPA al 50%) a causa della totale eliminazione del costo di ore straordinarie e della riduzione dei costi legati alle trasferte pari al 74,83%. Questo grado di automazione, infatti, permette di raccogliere in automatico i dati dall'ambiente IT aziendale per cui parte delle trasferte non è più svolta ad eccezione di quella relativa all'acquisizione cliente e al kick off iniziale volto alla conoscenza del sistema informativo aziendale. Vi è un parziale riassorbimento delle risorse: 8 internal developers assunti ma circa 27 dimessi per un totale di 19 risorse "perse". La composizione del costo totale risulta essere adesso pari al 42% lavoro e 58% capitale contro il 100% lavoro del caso iniziale e al 73% lavoro e 27% capitale del caso dell'RPA al 50%.
La riduzione del lavoro comporta un *Gross Savings= 1.820.860,34 €* che al netto dei costi legati all'automazione, quali le royalties pari al 10,5% del fatturato lordo, ai componenti IT e la maintenance, porta un *Net Savings= 848.265,34€.*

Nei due scenari possibili di automatizzazione si sono calcolati Payback, ROI e VAN per valutare la bontà dell'investimento. Nel calcolo dei 3 indici si sono considerati, per semplicità, flussi di cassa costanti nel tempo con un fattore di sconto pari a r=10%, come mostrato nell'allegato 13.
Il Payback ottenuto suggerirebbe un ritorno sull'investimento in RPA al 93% in 8-9 anni, un anno in meno rispetto ad una RPA pari al 50% il cui ritorno è in 5-6 anni, in quanto, nonostante l'investimento iniziale sia superiore, i Net Saving crescono, scontati al 10%, di più in proporzione. Ma il Payback period è un criterio di valutazione degli investimenti improprio in quanto evidenzia la rischiosità dell'investimento in termini temporali ma non dà alcuna informazione circa la redditività dei progetti, il valore temporale del denaro e dei flussi di cassa futuri.
Nel calcolo del ROI si sono considerati due scenari temporali.

Nel caso di un orizzonte temporale di 5 anni entrambe le forme di automazione presentano un ROI negativo (il Payback in entrambi i casi è superiore ai 5 anni) per cui anche il VAN calcolato sullo stesso periodo di 5 anni risulta negativo. I primi ritorni economici si hanno, dunque, dopo 5-6 anni dalla data di investimento.

In un orizzonte di 10 anni invece la situazione è diversa. Avendo superato il Payback time, i ritorni economici sull'investimento sono adesso positivi. L'RPA al 50% presenta infatti un ROI pari al 13% e un *VAN = 253.463,53€* mentre l'automazione al 93% presenta un ROI pari al 55% e un *VAN = 1.849.039,29€.* Dall'analisi degli *indici risulterebbe quindi maggiormente profittevole investire maggiormente in un RPA più "spinta".*

I benefici dell'RPA sono tanto maggiori quanto è maggiore il fatturato lordo dell'azienda. È importante considerare che, nella prima analisi, per semplicità, i fatturati sono stati considerati costanti nei 3 scenari, ma qualora fossero considerati crescenti grazie ad una maggiore efficienza dovuta all'adozione dell'RPA allora i benefici di quest'ultima sarebbero nettamente ampliati.

La maggior efficienza deriva da un'importante riduzione dei tempi dei progetti (del 50% e del 93% nei rispettivi casi) come mostrato nel grafico 13.

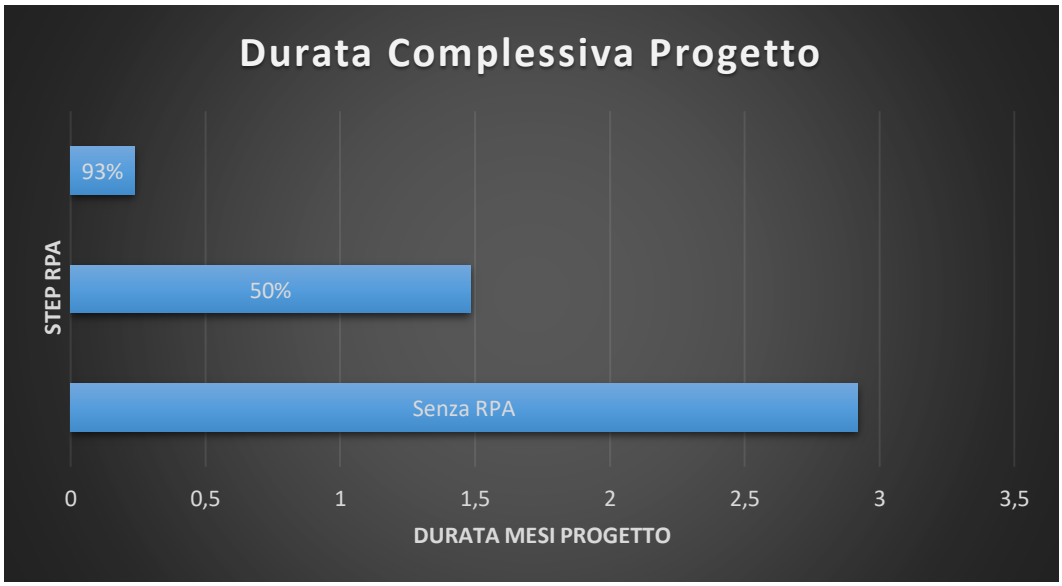


Grafico 16 Confronto durate

IMPATTO SULL'ORGANIZZAZIONE

L'impatto sull'organizzazione dei due scenari è molto differente.

Nel caso di automazione al 50%, essendo l'RPA a supporto dell'uomo, ma non sostitutiva ad esso, l'impatto sull'organizzazione non è così elevato da riformulare tutti i compiti. Secondo lo scenario analizzato, introducendo l'automazione parziale, l'organizzazione aziendale cambierebbe come mostrato di seguito:

Nuovo team con RPA 0,5	
Analyst I	9
Analyst II	3
Consultant	4
Senior Consultant	2
Manager	3
Partner	1
Process developers	4
Totale	**26**

7 Analyst I, 3 Analyst II, 1 Consultant,1 Senior Consultant e 1 Manager dovrebbero essere dismessi in quanto il loro lavoro non è più necessario. Sono assunti, invece, per compensare il carico 4 developers, più skillati tecnologicamente, per cui il team di lavoro si arricchisce di competenze diverse.

I developers hanno un ruolo determinante in ambito "maintenance & operations" poiché sebbene i robot siano configurati a partire da requisiti di business definiti, una più ampia architettura e modifiche ai sistemi possono influire pesantemente sulle prestazioni previste come modifiche ai campi in cui sono registrati i dati e integrazioni di sistema. Si rende necessario anche il monitoraggio delle capacità e delle prestazioni della macchina ed effettuare considerazioni sulla compatibilità a lungo termine.[42]

Le altre figure analyst I, analyst II, consultant, senior consultant, manager e partner non percepiscono cambiamenti nelle loro attività, possono però fare maggior reliance sull'output della macchina e velocizzare i rispettivi compiti.

Ben diverso è lo scenario con automazione al 93%, ovvero quasi totale. Esso prevede un significativo riassetto dell'organico aziendale, con l'automazione delle attività operative ripetitive. Tutte le figure, ad eccezione dei manager, non si rendono più

[42] EY, *Risk and Control considerations within RPA implementations* https://www.ey.com/Publication/vwLUAssets/EY-risk-and-control-considerations-within-RPA-implementations/$File/EY-risk-and-control-considerations-within-RPA-implementations.pdf

necessarie e sono rimpiazzate da una forza lavoro più skillata tecnologicamente a cui sono assegnati compiti diversi.

In questa forza lavoro rientrano figure quali:

- RPA architects, sono responsabili dell'analisi dei processi aziendali e dell'identificazione/attuazione delle soluzioni di automazione;
- Process developers, hanno il compito di specificare le istruzioni dettagliate che i robot devono eseguire e riportarle nel "robot controller repository";
- Robot Controller, hanno il compito di assegnare i lavori ai robot e monitorare le loro attività, analizzando le dashboard compilate automaticamente e i rischi associati al loro funzionamento come la cybersecurity.

In generale, l'investimento in RPA 93% risulta più profittevole in termini temporali ed economici in quanto un maggior grado di automazione eliminerebbe i problemi legati alle risorse visti ad inizio capitolo quali:

- sovrallocamento durante i periodi di picco, con il conseguente pagamento degli straordinari;
- I picchi di lavoro durante i fiscal year, consentendo all'azienda di acquisire più clienti vista la maggiore flessibilità ed efficienza;
- L'alto turnover delle risorse poco "skillate", con inserimento di risorse più competenti dal punto di vista tecnologico e con lo svolgimento delle attività poco complesse e molto ripetitive da parte della macchina

In aggiunta, un'RPA altamente automatizzata permetterebbe, una maggior qualità del report di revisione finale grazie alla maggior accuratezza della macchina nell'analisi dei dati.

Tuttavia, nel ricorrere a un'automazione così spinta, si generano tutta una serie di problemi da gestire, quali l'abuso di accessi privilegiati, mal gestione dei diritti di accesso e divulgazione dei dati sensibili. Si aggiungono, inoltre, la vulnerabilità della sicurezza della piattaforma, le implicazioni per la privacy dei clienti e la negazione del servizio che possono impattare sull'integrità e sull'affidabilità dell'RPA applicata al business process.

La scelta su quale tipo di automazione investire, dipende in definitiva dall'avversione al rischio che la società presenta e dalle procedure che intende mettere in atto per gestirlo.

CONCLUSIONI

Questo lavoro di tesi nasce dall'esperienza di tirocinio svolta presso la società di consulenza, per cui, per ragioni di riservatezza non si cita il nome. Il ruolo svolto durante questa esperienza è stato quello dell'IT Auditor, le cui attività sono state studiate per lo sviluppo del presente lavoro di tesi.

Nel primo capitolo si è data un'overview generale sulle ragioni per cui è effettuata la revisione contabile e sull'importanza della revisione del bilancio per la tutela degli stakeholders.

Nel secondo capitolo si è descritta nel dettaglio l'attività di auditing relativa all'ambiente IT, quindi tutte le procedure seguite, dalla compilazione dell'IT Understanding del cliente auditato al giudizio finale sul sistema di controllo interno relativo all'IT.

Nel terzo capitolo si è indagato su come un'automazione di tipo RPA (Robotic Process Automation) potrebbe impattare sul processo di revisione interna dell'ambiente IT sia termini organizzativi sia in termini di nuovi scenari di rischio emergenti dal nuovo scenario tecnologico.

È stato sviluppato infine un progetto applicativo su una società di revisione con l'obiettivo di evidenziare in una prima fase le criticità che impattano sul modello di business e successivamente attraverso un'analisi costi benefici, si è sperimentata l'applicazione di un software di RPA con due diversi stati di automazione e i suoi impatti sia sul processo di revisione della società presa in considerazione, sia sull'organizzazione di quest'ultima.

RIFERIMENTI BIBLIOGRAFICI E SITOGRAFIA

Deloitte, (2018) Internal control, A guide for auditors in DTTL member firms

Deloitte, (2018) IT Auditing

Roberto Ercoli, 19 Aprile 2019, Il controllo di qualita' nella revisione: normativa e novità, la REVISIONE LEGALE

Mirko Alchirafi, 2011, Tesi di Laurea in Economia e commercio, Indipendenza e conflitto d'interessi nella revisione legale dei conti: qualità ed evoluzione delle funzioni del revisore alla luce delle recenti riforme

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

Fonte D. Balducci, Tenere la contabilità, FAG, Milano, 2012.

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

Mirko Alchirafi, tesi di laurea, 2011, INDIPENDENZA E CONFLITTO D'INTERESSI NELLA REVISIONE LEGALE DEI CONTI: QUALITA' ED EVOLUZIONE DELLE FUNZIONI DEL REVISORE ALLA LUCE DELLE RECENTI RIFORME

Source Portale Deloitte, Tech Library

Natale Prampolini, La legge 262/05 e le sue implicazioni, 2011, AIEA

1 Decreto Legislativo 8 giugno 2001, n. 231, pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 2001

Obiettivi di controllo IT per il Sarbanes_Oxley Acr, 2° Edizione, settembre 2016

ASSIREVI, Gennaio 2019, Monografia COSO Framework

NTT DATA CONSULTING, LA ROBOTIC PROCESS AUTOMATION PER RIDURRE I COSTI DELLE OPERATIONS

Deloitte, 2017, Automate this The business leader's guide to robotic and intelligent automation

PWC, Robotic process automation: A primer for internal audit professionals

Bendig Bygstaf, The Coming of Lightweight IT, 29/05/2015,

Automate this: The business leader's guide to robotic and intelligent automation, Deloitte

https://www.pwc.com.au/risk-controls/technology-risk.html

https://www.smartsheet.com/understanding-it-compliance

https://www.pwc.com.au/risk-controls/technology-risk.html

https://www.eaca.eu/wp-content/uploads/2016/06/sarbanes.pdf

https://www.snowviewfarm.com/qual-e-il-public-company-accounting-oversight-board/

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

https://www.sarbanes-oxley-101.com/SOX-906.htm

https://www.sarbanes-oxley-101.com/SOX-404.htm
https://www.auditboard.com/sox-compliance/

https://www.ricercagiuridica.com/codici/vis.php?num=24786&search=

https://www.pwc.com/il/en/Advisory/compliance.html

http://www.carrtegra.com/2016/06/importance-internal-controls-accounting/

https://www.investopedia.com/terms/i/internalcontrols.asp

https://asq.org/quality-resources/auditing

https://www.bdo.it/it-it/services-it/advisory/digital-consulting/is-audit-compliance-support
https://www.siav.com/it/soluzioni-software/robotic-process-automation/
https://www.automationanywhere.com/solutions/attended-vs-unattended-rpa

http://www.cualeva.com/rpa-e-ia-tra-collaborazione-e-differenze/
https://st.ilsole24ore.com/art/SoleOnLine4/100-parole/Tecnologia/C/Consumerization.shtml

https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1021&context=ecis2015_cr

https://www.uipath.com/blog/rpa-improves-legal-compliance

https://www.eng.it/resources/whitepaper/doc/rpa/RPA_whitepaper_ita.pdf

https://idea.caseware.com/products/idea

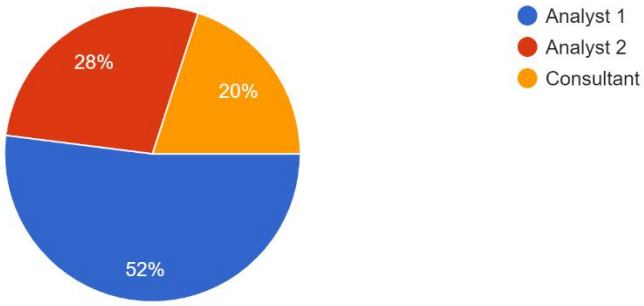
https://www.ey.com/Publication/vwLUAssets/EY-risk-and-control-considerations-within-RPA-implementations/$File/EY-risk-and-control-considerations-within-RPA-implementations.pdf

APPENDIX A

Questionario sottoposto ai dipendenti della società di consulenza X

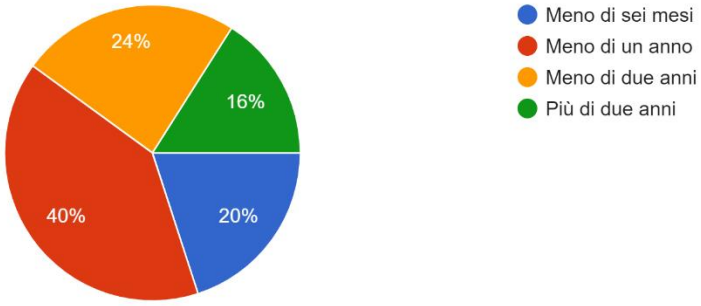
1. Qual è il tuo ruolo?

25 risposte



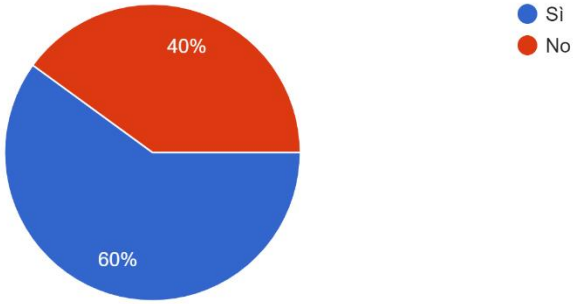
2. Da quanto tempo svolgi questa professione?

25 risposte



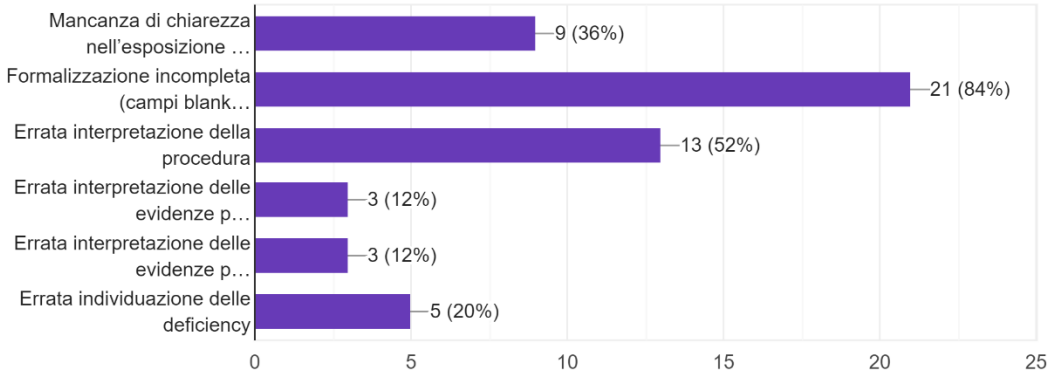
3. Sei alla ricerca attiva di un altro impiego?

25 risposte



4. Quali sono gli errori che emergono più spesso dalla review giornaliera? Inserisci una o più risposte

25 risposte

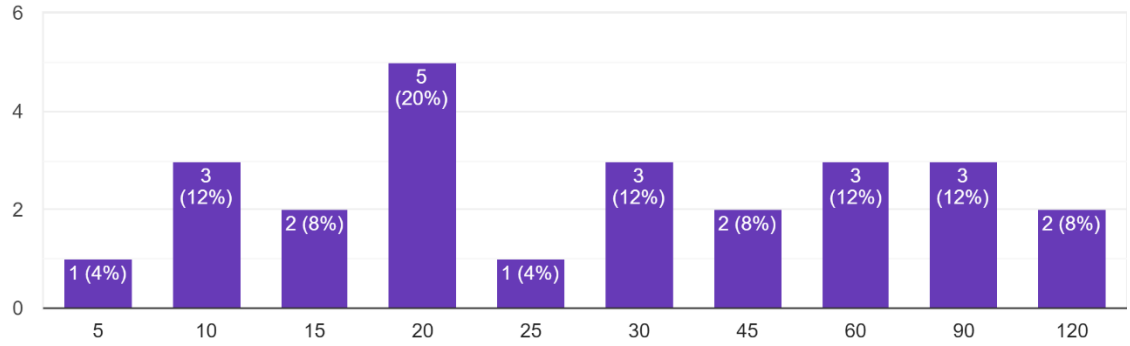


5. Qual è la causa principale degli errori che commetti?

25 risposte

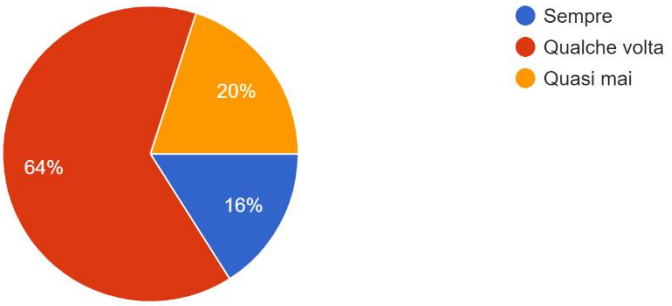
6. Dopo la review giornaliera, quanto tempo impieghi in media a correggere gli errori?

25 risposte



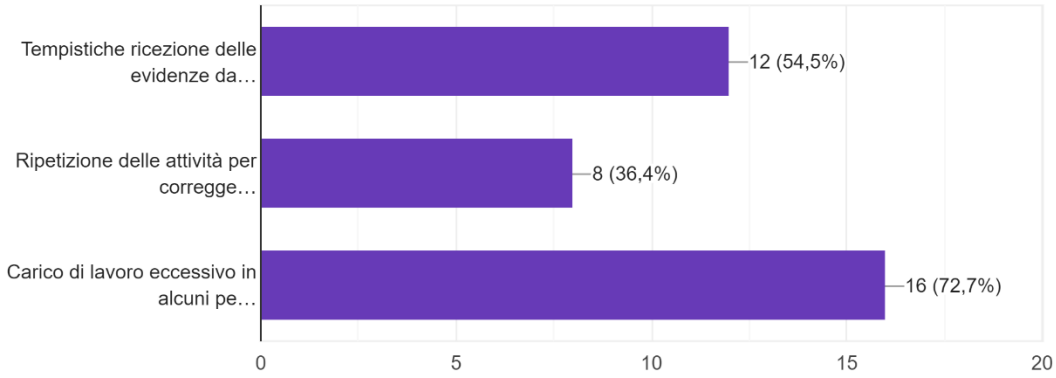
7. Quanto spesso riesci a rispettare le deadline?

25 risposte



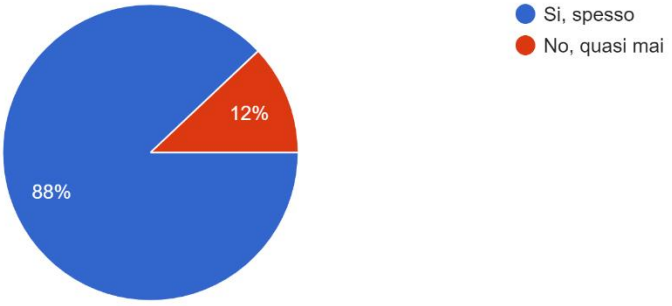
8. Se alla domanda precedente hai risposto qualche volta o quasi mai, qual è il motivo del ritardo?

22 risposte



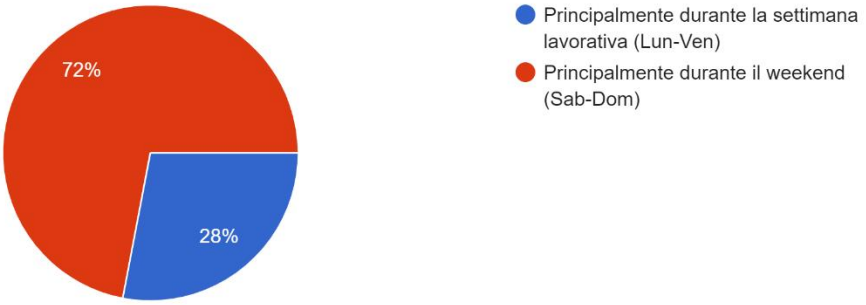
9. Ti capita di fare straordinario?

25 risposte



10. Quando fai straordinario?

25 risposte



Appendix B

COCOMO sta per Constructive Cost Model, ed è un modello che si basa sullo studio di centinaia di progetti software e utilizza un set di 17 driver di costo e 5 scale factors.

Applicando l'Equazione dello sforzo, si ricava il numero di person-month necessari per lo sviluppo del progetto in funzione degli SLOC, ovvero delle logical line of code da sviluppare stimate. Ci sono diversi modi per stimare le nuove linee di codice. La fonte migliore è quella dei dati storici. Una linea di codice sorgente è generalmente intesa ad escludere i software di supporto non consegnati, come i test driver. Per esempio, non sono inclusi nella definizione i software commerciali off-the-shelf (COTS), i software governativi (GFS), altri prodotti, le librerie di supporto linguistico e i sistemi operativi, o altre librerie commerciali. Il codice generato con i generatori di codice sorgente viene gestito contando le direttive di operatori separati come linee di codice sorgente.

Dall'equazione dello sforzo si ricava il Development Time e il numero di developer necessari.

$$E = A * (KSLOC)^{1,01+0,01*\sum SF} * EAF$$

$$D(E) = 3E^{0,33+0,2*(B-0,01)} * \frac{SCED\%}{100}$$

$$Staff\ size = \frac{E}{D(E)}$$

Per la stima dell'effort si considerano gli scale factor vanno a definire il Process Risk e determinano l'esponente dell'effort $B = 1,01 + 0,01 * \sum SF$ che descrive la SIZE. Essi sono:

Scaling Factors	**Description**
Precedentedness	Reflects the previous experience of the organization
Development Flexibility	Reflects the degree of flexibility in the development process
Architecture/ Risk Resolution	Reflects the extent of risk analysis carried out
Team Cohesion	Reflects how well the development team knows each other and work together

Process Maturity	Reflects the process maturity of the organization

- Se l'esponente B>1 il progetto mostra diseconomie di scala. Ciò è dovuto in generale a due fattori principali: la crescita delle comunicazioni interpersonali e la crescita dell'integrazione di sistemi di grandi dimensioni. I progetti più grandi avranno più personale, e quindi più percorsi di comunicazione interpersonale che consumeranno le spese generali. L'integrazione di un piccolo prodotto come parte di un prodotto più grande richiede non solo lo sforzo per sviluppare il piccolo prodotto, ma anche lo sforzo aggiuntivo di overhead per progettare, mantenere, integrare e testare le sue interfacce con il resto del prodotto.
- Se B = 1,0, le economie e le diseconomie di scala sono in equilibrio. Questo modello lineare è spesso utilizzato per la stima dei costi di piccoli progetti.
- Se B < 1.0, il progetto presenta economie di scala. Se la dimensione del prodotto è raddoppiata, lo sforzo del progetto è meno che raddoppiato. La produttività del progetto aumenta con l'aumento delle dimensioni del prodotto.

I cost driver che impattano sull'effort da utilizzare per lo sviluppo di un software sono 17 e vanno a definire l'Effort Adjustment Factor $EAF = PRODUTTORIA\ CF$.

Tutti i driver di costo hanno livelli di valutazione qualitativa (da "extra low" a "extra high") che esprimono l'impatto del driver e un moltiplicatore di sforzo corrispondente. Il livello nominale ha sempre un moltiplicatore di sforzo (EM) di 1,00, che non cambia lo sforzo stimato. Quindi per l'utilizzo nel modello la valutazione qualitativa di un fattore di costo si traduce in una valutazione quantitativa. [43]

I cost driver sono divisi in base al tipo di rischio che descrivono. Le categorie di rischio sono:

- Product Risk: è correlato all'affidabilità richiesta del prodotto software (RELY), la dimensione del sofware (SIZE), la complessità del prodotto (CPLX), la dimensione del database (DATA) e dalla documentazione richiesta (DOCU).
- Reuse Risk è legato all'impatto del riutilizzo di un'applicazione (RUSE) nello sviluppo di software, che dipenderà dalla strategia di riutilizzo che richiede

[43] https://www.researchgate.net/publication/243482239_Cocomo_ii_model_definition_manual

affidabilità, esperienza e strumenti adeguati per garantire il successo di un prodotto

- Platform Risk: è legato alla volatilità della piattaforma di sviluppo (PVOL) che potrebbe introdurre problemi nel futuro con la necessità di rielaborare alcune fasi del progetto (TIME e STOR).
- Personnel Risk: è la fonte primaria dei rischi del progetto e influisce sulla produttività complessiva di un progetto di sviluppo software. Il rischio del personale è legato alla continuità del personale (PCON), alla capacità degli analyst (ACAP) e all'esperienza complessiva (AEXP) così come all'esperienza dei programmatori con il particolare linguaggio di programmazione e i tool utilizzati (LTEX) e le loro capacità (PCAP).
- Project Risk: emergerà se un progetto con un programma tight è stato sviluppato da uno o più sviluppatori con non elevata capacità tecnica. (SCED required development schedule)

  È influenzato dall'utilizzo di software tool (TOOL) e dallo sviluppo multisite (SITE).

17 COST DRIVERS	
I Product Attributes	
RELY	Required software reliability
DATA	Database size
CPLX	Product complexity
RUSE	Required percentage of reusable components
DOCU	Extent of documentation required
II Computer Attributes	
TIME	Execution time constraint
STOR	Main storage constraint
PVOL	Volatility of development platform
III Personnel Attributes	
ACAP	Project Analyst Capability
PCAP	Programmer capability
PCON	Personnel Continuity
APEX	Application experience
PLEX	Platform Experience
LTEX	Language and tool experience
IV Project Attributes	
TOOL	Use of software tools
SITE	Extent of multisite working and quality of inter-site communication
SCED	Required development schedule

ALLEGATO 1

PROGETTO PICCOLO SENZA RPA

TASK	Descrizione lavoro	Partner	Manager	Senior Consultant	Consultant	Analyst 2	Analyst 1	Total hours	Gross Fees	Ore Consultant per attività
Rate (ora)		450,00 €	240,00 €	190,00 €			70,00 €	84	10.200,00 €	64
		4	8	12			60			
Understanding IT Environment		3	4	2			6	15	3110	19,44
Partner	Rilevazione ed aggiornamento ambiente IT che caratterizza il gruppo X. (Acquisizione cliente, kick off e raccolta dati)	3						3	1.350	
Manager			4					4	960	
Senior Consultant				2				2	380	
Analyst 2								0	-	
Analyst 1							6	6	420	
GITC		1	4	10			54	69	7.090	44,31
Partner	Svolgimento dei controlli generali IT sugli applicativi CORE di X 4 Applicativi(con ridotto numero di controlli) + DB + OS + AD	1						1	450	
Manager			4					4	960	
Senior Consultant				10				10	1.900	
Consultant								0	-	
Analyst 2								0	-	
Analyst 1							54	54	3.780	
ITAC		0	0	0			0	0	-	0,00
Partner	Controlli automatici	0						0	-	
Manager			0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	
INTERFACCE		0	0	0			0	0	-	0,00
Manager	Analisi interfacce		0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	
IPE		0	0	0			0	0	-	0,00
Manager	IPE		0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	
Journal Entries Test		0	0	0			0	0	-	0,00

Manager	JET		0					0	-	
Analyst 1							0	0	-	
DATAWAREHOUSE		0	0	0			0	0	0	0,00
Partner	Analisi Datawarehouse	0						0	-	
Manager			0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	

Ruolo	RAL	RAL+TASSE	Costo orario risorsa	Ore lavorate	Rate orario	Ricavo totale	Peso	Costo Totale	Peso	Margine totale
ANALYST	25.000,00 €	33.750,00 €	16,67 €	60	70,00	4.200,00 €	41,18%	1.000,49 €	57,92%	3.199,51 €
ANALYST 2	28.000,00 €	37.800,00 €	18,68 €	0	85,00	0,00 €	0,00%	0,00 €	0,00%	0,00 €
Consultant	30.000,00 €	40.500,00 €	20,01 €	0	160,00	0,00 €	0,00%	0,00 €	0,00%	0,00 €
Senior Consu	37.500,00 €	50.625,00 €	25,01 €	12	190,00	2.280,00 €	22,35%	300,15 €	17,37%	1.979,85 €
MANAGER	45.000,00 €	60.750,00 €	30,01 €	8	240,00	1.920,00 €	18,82%	240,12 €	13,90%	1.679,88 €
PARTNER	70.000,00 €	94.500,00 €	46,69 €	4	450,00	1.800,00 €	17,65%	186,76 €	10,81%	1.613,24 €
Totale				**84**		**10.200,00 €**		**1.727,52 €**		**8.472,48 €**

ALLEGATO 2

PROGETTO MEDIO SENZA RPA

TASK	Descrizione lavoro	Partner	Manager	Senior Consultant	Consultant	Analyst 2	Analyst 1	Total hours	Gross Fees	Ore Consultant per attività
Rate (ora)		450,00 €	240,00 €	190,00 €	160,00 €	85,00 €	70,00 €	470	55.560,00 €	347
		6	50	24	88	72	230			
Understanding IT Environment		2	10	8	0	4	12	36	6000	37,50
Partner	Rilevazione ed aggiornamento ambiente IT che caratterizza il gruppo Y.	2						2	900	
Manager			10					10	2.400	
Senior Consultant				8				8	1.520	
Analyst 2						4		4	340	
Analyst 1							12	12	840	
GITC		2	24	16	88	32	140	302	36.300	226,88
Partner	Svolgimento dei controlli generali IT sugli applicativi CORE di Y (12 Applicativi + DB + OS + AD)	2						2	900	
Manager			24					24	5.760	
Senior Consultant				16				16	3.040	
Consultant					88			88	14.080	
Analyst 2						32		32	2.720	
Analyst 1							140	140	9.800	
ITAC		2	14	0	0	28	60	104	10.840	67,75
Partner	Controlli automatici	2						2	900	
Manager			14					14	3.360	
Analyst 2						28		28	2.380	
Analyst 1							60	60	4.200	
INTERFACCE		0	0	0	0	0	0	0	-	0,00
Manager	Analisi interfacce		0					0	-	
Analyst 2						0		0	-	
Analyst 1							0	0	-	
IPE		0	2	0	0	8	18	28	2.420	15,13
Manager	IPE		2					2	480	
Analyst 2						8		8	680	
Analyst 1							18	18	1.260	
Journal Entries Test		0	0	0	0	0	0	0	-	0,00
Manager	JET		0					0	-	
Analyst 1							0	0	-	

DATAWAREHOUSE		0	0	0	0	0	0	0	0	0,00
Partner	Analisi Datawharehouse	0						0	-	
Manager			0					0	-	
Analyst 2						0		0	-	
Analyst 1							0	0	-	

Ruolo	RAL	RAL+TASSE	Costo orario risorsa	Ore lavorate	Rate orario	Ricavo totale	Peso	Costo Totale	Peso	Margine totale
ANALYST	25.000,00 €	33.750,00 €	16,67 €	230	70,00	16.100,00 €	28,98%	3.835,23 €	41,14%	12.264,77 €
ANALYST 2	28.000,00 €	37.800,00 €	18,68 €	72	85,00	6.120,00 €	11,02%	1.344,66 €	14,42%	4.775,34 €
Consultant	30.000,00 €	40.500,00 €	20,01 €	88	160,00	14.080,00 €	25,34%	1.760,87 €	18,89%	12.319,13 €
Senior Consu	37.500,00 €	50.625,00 €	25,01 €	24	190,00	4.560,00 €	8,21%	600,30 €	6,44%	3.959,70 €
MANAGER	45.000,00 €	60.750,00 €	30,01 €	50	240,00	12.000,00 €	21,60%	1.500,74 €	16,10%	10.499,26 €
PARTNER	70.000,00 €	94.500,00 €	46,69 €	6	450,00	2.700,00 €	4,86%	280,14 €	3,01%	2.419,86 €
Totale				**470**		**55.560,00 €**		**9.321,94 €**		**46.238,06 €**

ALLEGATO 3

PROGETTO GRANDE SENZA RPA

TASK	Descrizione lavoro	Partner	Manager	Senior Consultant	Consultant	Analyst 2	Analyst 1	Total hours	Gross Fees	Ore Consultant per attività
Rate (ora)		450,00 €	240,00 €	190,00 €	160,00 €	85,00 €	70,00 €	1464	138.640,00 €	867
		12	80	34	108	280	950			
Understanding IT Environment		5	8	8	0	10	20	51	7940	49,63
Partner	Rilevazione ed aggiornamento ambiente IT che caratterizza il gruppo Z.	5						5	2.250	
Manager			8					8	1.920	
Senior Consultant				8				8	1.520	
Analyst 2						10		10	850	
Analyst 1							20	20	1.400	
GITC		4	40	26	108	152	380	710	73.140	457,13
Partner	Svolgimento dei controlli generali IT sugli applicativi CORE di Z (23 Applicativi + DB + OS + AD)	4						4	1.800	
Manager			40					40	9.600	
Senior Consultant				26				26	4.940	
Consultant					108			108	17.280	
Analyst 2						152		152	12.920	
Analyst 1							380	380	26.600	
ITAC		2	15	0	0	50	180	247	21.350	133,44
Partner	Controlli automatici	2						2	900	
Manager			15					15	3.600	
Analyst 2						50		50	4.250	
Analyst 1							180	180	12.600	
INTERFACCE		0	5	0	0	20	50	75	6.400	40,00
Manager	Analisi interfacce		5					5	1.200	
Analyst 2						20		20	1.700	
Analyst 1							50	50	3.500	
IPE		0	4	0	0	24	78	106	8.460	52,88
Manager	IPE		4					4	960	
Analyst 2						24		24	2.040	
Analyst 1							78	78	5.460	
Journal Entries Test		0	4	0	0	0	180	184	13.560	84,75
Manager	12 JET		4					4	960	
Analyst 1							180	180	12.600	

DATAWAREHOUSE		1	4	0	0	24	62	91	7790	48,69
Partner	Analisi Datawharehouse	1						1	450	
Manager			4					4	960	
Analyst 2						24		24	2.040	
Analyst 1							62	62	4.340	

Ruolo	RAL	RAL+TASSE	Costo orario risorsa	Ore lavorate	Rate orario	Ricavo totale	Peso	Costo Totale	Peso	Margine totale
ANALYST	25.000,00 €	33.750,00 €	16,67 €	950	70,00	66.500,00 €	47,97%	15.841,16 €	58,58%	50.658,84 €
ANALYST 2	28.000,00 €	37.800,00 €	18,68 €	280	85,00	23.800,00 €	17,17%	5.229,25 €	19,34%	18.570,75 €
Consultant	30.000,00 €	40.500,00 €	20,01 €	108	160,00	17.280,00 €	12,46%	2.161,07 €	7,99%	15.118,93 €
Senior Consu	37.500,00 €	50.625,00 €	25,01 €	34	190,00	6.460,00 €	4,66%	850,42 €	3,14%	5.609,58 €
MANAGER	45.000,00 €	60.750,00 €	30,01 €	80	240,00	19.200,00 €	13,85%	2.401,19 €	8,88%	16.798,81 €
PARTNER	70.000,00 €	94.500,00 €	46,69 €	12	450,00	5.400,00 €	3,89%	560,28 €	2,07%	4.839,72 €
Totale				**1464**		**138.640,00 €**		**27.043,35 €**		**111.596,65 €**

ALLEGATO 4

PROGETTO PICCOLO CON RPA 0,5

TASK	Descrizione lavoro	Partner	Manager	Senior Consultant	Consultant	Analyst 2	Analyst 1	Total hours	Gross Fees	Ore Consultant per attività
Rate (ora)		450,00 €	240,00 €	190,00 €	160,00 €	85,00 €	70,00 €	46,5	6.445,00 €	40
		3,5	6	7	0	0	30			
Understanding IT Environment		3	4	2	0	0	3	12	2900	18,13
Partner	Rilevazione ed aggiornamento ambiente IT che caratterizza il gruppo X. (Acquisizione cliente, kick off e raccolta dati)	3						3	1.350	
Manager			4					4	960	
Senior Consultant				2				2	380	
Analyst 2								0	-	
Analyst 1							3	3	210	
GITC		0,5	2	5			27	34,5	3.545	22,16
Partner	Svolgimento dei controlli generali IT sugli applicativi CORE di X 4 Applicativi(con ridotto numero di controlli) + DB + OS + AD	0,5						0,5	225	
Manager			2					2	480	
Senior Consultant				5				5	950	
Consultant								0	-	
Analyst 2								0	-	
Analyst 1							27	27	1.890	
ITAC		0	0	0			0	0	-	0,00
Partner	Controlli automatici	0						0	-	
Manager			0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	
INTERFACCE		0	0	0			0	0	-	0,00
Manager	Analisi interfacce		0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	
IPE		0	0	0			0	0	-	0,00
Manager	IPE		0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	
Journal Entries Test		0	0	0			0	0	-	0,00

Manager	12 JET		0					0	-	
Analyst 1							0	0	-	
DATAWAREHOUSE		0	0	0			0	0	0	0,00
Partner	Analisi Datawarehouse	0						0	-	
Manager			0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	

Ruolo	RAL	RAL+TASSE	Costo orario risorsa	Ore lavorate	Rate orario	Ricavo totale	Peso	Costo Totale	Peso	Margine totale
ANALYST	25.000,00 €	33.750,00 €	16,67 €	30	70,00 €	4.200,00 €	41,18%	500,25 €	49,10%	3.699,75 €
ANALYST 2	28.000,00 €	37.800,00 €	18,68 €	0	85,00 €	0,00 €	0,00%	0,00 €	0,00%	0,00 €
Consultant	30.000,00 €	40.500,00 €	20,01 €	0	160,00 €	0,00 €	0,00%	0,00 €	0,00%	0,00 €
Senior Consu	37.500,00 €	50.625,00 €	25,01 €	7	190,00 €	2.280,00 €	22,35%	175,09 €	17,18%	2.104,91 €
MANAGER	45.000,00 €	60.750,00 €	30,01 €	6	240,00 €	1.920,00 €	18,82%	180,09 €	17,68%	1.739,91 €
PARTNER	70.000,00 €	94.500,00 €	46,69 €	3,5	450,00 €	1.800,00 €	17,65%	163,41 €	16,04%	1.636,59 €
Totale				**46,5**		**10.200,00 €**		**1.018,84 €**		**9.181,16 €**

ALLEGATO 5

PROGETTO MEDIO CON RPA 0,5

TASK	Descrizione lavoro	Partner	Manager	Senior Consultant	Consultant	Analyst 2	Analyst 1	Total hours	Gross Fees	Ore Consultant per attività
Rate (ora)		450,00 €	240,00 €	190,00 €	160,00 €	85,00 €	70,00 €	245	30.190,00 €	189
		4	30	16	44	36	115			
Understanding IT Environment		2	10	8	0	2	6	28	5410	33,81
Partner	Rilevazione ed aggiornamento ambiente IT che caratterizza il gruppo Y.	2						2	900	
Manager			10					10	2.400	
Senior Consultant				8				8	1.520	
Analyst 2						2		2	170	
Analyst 1							6	6	420	
GITC		1	12	8	44	16	70	151	18.150	113,44
Partner	Svolgimento dei controlli generali IT sugli applicativi CORE di Y (12 Applicativi + DB + OS + AD)	1						1	450	
Manager			12					12	2.880	
Senior Consultant				8				8	1.520	
Consultant					44			44	7.040	
Analyst 2						16		16	1.360	
Analyst 1							70	70	4.900	
ITAC		1	7	0	0	14	30	52	5.420	33,88
Partner	Controlli automatici	1						1	450	
Manager			7					7	1.680	
Analyst 2						14		14	1.190	
Analyst 1							30	30	2.100	
INTERFACCE		0	0	0	0	0	0	0	-	0,00
Manager	Analisi interfacce		0					0	-	
Analyst 2						0		0	-	
Analyst 1							0	0	-	
IPE		0	1	0	0	4	9	14	1.210	7,56
Manager	IPE		1					1	240	
Analyst 2						4		4	340	
Analyst 1							9	9	630	
Journal Entries Test		0	0	0	0	0	0	0	-	0,00
Manager	JET		0					0	-	
Analyst 1							0	0	-	

DATAWAREHOUSE		0	0	0	0	0	0	0	0	0,00
Partner	Analisi Datawharehouse	0						0	-	
Manager			0					0	-	
Analyst 2						0		0	-	
Analyst 1							0	0	-	

Ruolo	RAL	RAL+TASSE	Costo orario risorsa	Ore lavorate	Rate orario	Ricavo totale	Peso	Costo Totale	Peso	Margine totale
ANALYST	25.000,00 €	33.750,00 €	16,67 €	115	70,00	16.100,00 €	28,98%	1.917,61 €	38,68%	14.182,39 €
ANALYST 2	28.000,00 €	37.800,00 €	18,68 €	36	85,00	6.120,00 €	11,02%	672,33 €	13,56%	5.447,67 €
Consultant	30.000,00 €	40.500,00 €	20,01 €	44	160,00	14.080,00 €	25,34%	880,43 €	17,76%	13.199,57 €
Senior Consu	37.500,00 €	50.625,00 €	25,01 €	16	190,00	4.560,00 €	8,21%	400,20 €	8,07%	4.159,80 €
MANAGER	45.000,00 €	60.750,00 €	30,01 €	30	240,00	12.000,00 €	21,60%	900,44 €	18,16%	11.099,56 €
PARTNER	70.000,00 €	94.500,00 €	46,69 €	4	450,00	2.700,00 €	4,86%	186,76 €	3,77%	2.513,24 €
Totale				**245**		**55.560,00 €**		**4.957,78 €**		**50.602,22 €**

ALLEGATO 6

PROGETTO GRANDE CON RPA 0,5

TASK	Descrizione lavoro	Partner	Manager	Senior Consultant	Consultant	Analyst 2	Analyst 1	Total hours	Gross Fees	Ore Consultant per attività
Rate (ora)		450,00 €	240,00 €	190,00 €	160,00 €	85,00 €	70,00 €	751,5	74.430,00 €	465
		9	52,5	21	54	140	475			
Understanding IT Environment		5	8	8	0	5	10	36	6815	42,59
Partner	Rilevazione ed aggiornamento ambiente IT che caratterizza il gruppo Z.	5						5	2.250	
Manager			8					8	1.920	
Senior Consultant				8				8	1.520	
Analyst 2						5		5	425	
Analyst 1							10	10	700	
GITC		2	20	13	54	76	190	355	36.570	228,56
Partner	Svolgimento dei controlli generali IT sugli applicativi CORE di Z (23 Applicativi + DB + OS + AD)	2						2	900	
Manager			20					20	4.800	
Senior Consultant				13				13	2.470	
Consultant					54			54	8.640	
Analyst 2						76		76	6.460	
Analyst 1							190	190	13.300	
ITAC		1	7,5	0	0	25	90	123,5	10.675	66,72
Partner	Controlli automatici	1						1	450	
Manager			7,5					7,5	1.800	
Analyst 2						25		25	2.125	
Analyst 1							90	90	6.300	
INTERFACCE		0	5	0	0	10	25	40	3.800	23,75
Manager	Analisi interfacce		5					5	1.200	
Analyst 2						10		10	850	
Analyst 1							25	25	1.750	
IPE		0	4	0	0	12	39	55	4.710	29,44
Manager	IPE		4					4	960	
Analyst 2						12		12	1.020	
Analyst 1							39	39	2.730	
Journal Entries Test		0	4	0	0	0	90	94	7.260	45,38
Manager	12 JET		4					4	960	
Analyst 1							90	90	6.300	

DATAWAREHOUSE		1	4	0	0	12	31	48	4600	28,75
Partner	Analisi Datawharehouse	1						1	450	
Manager			4					4	960	
Analyst 2						12		12	1.020	
Analyst 1							31	31	2.170	

Ruolo	RAL	RAL+TASSE	Costo orario risorsa	Ore lavorate	Rate orario	Ricavo totale	Peso	Costo Totale	Peso	Margine totale
ANALYST	25.000,00 €	33.750,00 €	16,67 €	475	70,00	66.500,00 €	47,97%	7.920,58 €	56,03%	58.579,42 €
ANALYST 2	28.000,00 €	37.800,00 €	18,68 €	140	85,00	23.800,00 €	17,17%	2.614,62 €	18,49%	21.185,38 €
Consultant	30.000,00 €	40.500,00 €	20,01 €	54	160,00	17.280,00 €	12,46%	1.080,53 €	7,64%	16.199,47 €
Senior Consultant	37.500,00 €	50.625,00 €	25,01 €	21	190,00	6.460,00 €	4,66%	525,26 €	3,72%	5.934,74 €
MANAGER	45.000,00 €	60.750,00 €	30,01 €	52,5	240,00	19.200,00 €	13,85%	1.575,78 €	11,15%	17.624,22 €
PARTNER	70.000,00 €	94.500,00 €	46,69 €	9	450,00	5.400,00 €	3,89%	420,21 €	2,97%	4.979,79 €
Totale				**751,5**		**138.640,00 €**		**14.136,98 €**		**124.503,02 €**

ALLEGATO 7

Calcolo costi e tempi di sviluppo per automazione 0,5

Scaling Factors	very Low	Low	Nominal	High	Very High	Extra High
Precedentedness	6,2	4,96	3,72	2,48	1,24	
Development Flexibility	5,07	4,05	3,04	2,03	1,01	
Architecture/ Risk Resolution	7,07	5,65	4,24	2,83	1,41	
Team Cohesion	5,48	4,38	3,29	2,19	1,1	
Process Maturity	7,8	6,24	4,68	3,12	1,56	

$B = 1{,}01 + 0{,}01 * \sum SF$ =1,16 essendo esso maggiore di 1 esplica la presenza di diseconomie di scala.

COST DRIVER	*VERY LOW*	*LOW*	*NOMINAL*	*HIGH*	*VERY HIGH*	*EXTRA HIGH*
Prod.Attr						
RELY	0,82	0,92	1,00	1,10	1,26	
DATA		0,90	1,00	1,14	1,28	
CPLX	0,73	0,87	1,00	1,17	1,34	
RUSE		0,95	1,00	1,07	1,15	
DOCU	0,81	0,91	1,00	1,11	1,23	
Comp.Attr						
TIME			1,00	1,11	1,29	1,63
STOR			1,00	1,05	1,17	1,46
PVOL		0,87	1,00	1,15	1,30	
Pers.Attr.						
ACAP	1,42	1,22	1,00	0,85	0,71	
PCAP	1,34	1,16	1,00	0,88	0,76	
PCON	1,29	1,10	1,00	0,9	0,81	
APEX	1,22	1,10	1,00	0,88	0,81	
PLEX	1,19	1,12	1,00	0,91	0,85	
LTEX	1,20	1,10	1,00	0,91	0,84	
Project Attr.						
TOOL	1,17	1,09	1,00	0,90	0,78	
SITE	1,22	1,09	1,00	0,93	0,86	0,8
SCED	1,43	1,14	1,00	1,00	1,00	

EAF= PROD(CD)= 0,36

ALLEGATO 8

PROGETTO PICCOLO CON RPA 0,93

TASK	Descrizione lavoro	Partner	Manager	Senior Consultant	Consultant	Analyst 2	Analyst 1	Total hours	Gross Fees	Ore Consultant per attività
Rate (ora)		450,00 €	240,00 €	190,00 €	160,00 €	85,00 €	70,00 €	14,000	3.190,67 €	20
		3,07	**4,27**	**2,67**			**4**			
Understanding IT Environment		3,00	4,00	2,00	0,00	0,00	0,40	9,40	2718,00	16,99
Partner	Rilevazione ed aggiornamento ambiente IT che caratterizza il gruppo X.	3,00						3,00	1350,00	
Manager			4,00					4,00	960,00	
Senior Consultant				2,00				2,00	380,00	
Analyst 2								0,00	0,00	
Analyst 1							0,40	0,40	28,00	
GITC		0,07	0,27	0,67	0,00	0,00	3,60	4,60	472,67	2,95
Partner	Svolgimento dei controlli generali IT sugli applicativi CORE di X 4 Applicativi(con ridotto numero di controlli) + DB + OS + AD	0,07						0,07	30,00	
Manager			0,27					0,27	64,00	
Senior Consultant				0,67				0,67	126,67	
Consultant								0,00	0,00	
Analyst 2								0,00	0,00	
Analyst 1							3,60	3,60	252,00	
ITAC		0	0	0	0	0	0	0	-	0,00
Partner	Controlli automatici	0						0	-	
Manager			0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	
INTERFACCE		0	0	0	0	0	0	0	-	0,00
Manager	Analisi interfacce		0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	
IPE		0	0	0	0	0	0	0	-	0,00
Manager	IPE		0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	
Journal Entries Test		0	0	0	0	0	0	0	-	0,00
Manager	JET		0					0	-	
Analyst 1							0	0	-	
DATAWAREHOUSE		0	0	0	0	0	0	0	0	0,00
Partner	Analisi Datawarehouse	0						0	-	

Manager			0					0	-	
Analyst 2								0	-	
Analyst 1							0	0	-	

Ruolo	RAL	RAL+TASSE	Costo orario risorsa	Ore lavorate	Rate orario	Ricavo totale	Peso	Costo Totale	Peso	Margine totale
ANALYST	25.000,00 €	33.750,00 €	16,67 €	4	70,00	4.200,00 €	41,18%	66,70 €	16,48%	4.133,30 €
ANALYST 2	28.000,00 €	37.800,00 €	18,68 €	0	85,00	0,00 €	0,00%	0,00 €	0,00%	0,00 €
Consultant	30.000,00 €	40.500,00 €	20,01 €	0	160,00	0,00 €	0,00%	0,00 €	0,00%	0,00 €
Senior Consultant	37.500,00 €	50.625,00 €	25,01 €	2,67	190,00	2.280,00 €	22,35%	66,70 €	16,48%	2.213,30 €
MANAGER	45.000,00 €	60.750,00 €	30,01 €	4,27	240,00	1.920,00 €	18,82%	128,06 €	31,65%	1.791,94 €
PARTNER	70.000,00 €	94.500,00 €	46,69 €	3,07	450,00	1.800,00 €	17,65%	143,18 €	35,38%	1.656,82 €
Totale				**14,00**		**10.200,00 €**		**404,64 €**		**9.795,36 €**

ALLEGATO 9

PROGETTO MEDIO CON RPA 0,93

TASK	Descrizione lavoro	Partner	Manager	Senior Consultant	Consultant	Analyst 2	Analyst 1	Total hours	Gross Fees	Ore Consultant per attività
Rate (ora)		450,00 €	240,00 €	190,00 €	160,00 €	85,00 €	70,00 €	50	8.202,67 €	51
		2,27	**12,67**	**9,07**	**5,87**	**4,80**	**15,33**			
Understanding IT Environment		2,00	10,00	8,00	0,00	0,27	0,80	21,07	4898,666667	30,62
Partner	Rilevazione ed aggiornamento ambiente IT che caratterizza il gruppo Y.	2,00						2,00	900	
Manager			10,00					10,00	2.400	
Senior Consultant				8,00				8,00	1.520	
Analyst 2						0,27		0,27	23	
Analyst 1							0,80	0,80	56	
GITC		0,13	1,60	1,07	5,87	2,13	9,33	20,13	2.420	15,13
Partner	Svolgimento dei controlli generali IT sugli applicativi CORE di Y (12 Applicativi + DB + OS + AD)	0,13						0,13	60	
Manager			1,60					1,60	384	
Senior Consultant				1,07				1,07	203	
Consultant					5,87			5,87	939	
Analyst 2						2,13		2,13	181	
Analyst 1							9,33	9,33	653	
ITAC		0,13	0,93	0,00	0,00	1,87	4,00	6,93	723	4,52
Partner	Controlli automatici	0,13						0,13	60	
Manager			0,93					0,93	224	
Analyst 2						1,87		1,87	159	
Analyst 1							4,00	4,00	280	
INTERFACCE		0	0	0	0	0	0	0	-	0,00
Manager	Analisi interfacce		0					0	-	
Analyst 2						0		0	-	
Analyst 1							0	0	-	
IPE		0	0,13	0,00	0,00	0,53	1,20	1,87	161	1,01
Manager	IPE		0,13					0,13	32	
Analyst 2						0,53		0,53	45	
Analyst 1							1,20	1,20	84	
Journal Entries Test		0	0	0	0	0	0	0	-	0,00
Manager	JET/APP CoGe		0					0	-	

Analyst I							0	0	-	
DATAWAREHOUSE		0	0	0	0	0	0	0	0	0,00
Partner	Analisi Datawharehouse	0						0	-	
Manager			0					0	-	
Analyst 2						0		0	-	
Analyst I							0	0	-	

Ruolo	RAL	RAL+TASSE	Costo orario risorsa	Ore lavorate	Rate orario	Ricavo totale	Peso	Costo Totale	Peso	Margine totale
ANALYST	25.000,00 €	33.750,00 €	16,67 €	15,33	70,00	16.100,00 €	28,98%	255,68 €	21,75%	15.844,32 €
ANALYST 2	28.000,00 €	37.800,00 €	18,68 €	4,80	85,00	6.120,00 €	11,02%	89,64 €	7,63%	6.030,36 €
Consultant	30.000,00 €	40.500,00 €	20,01 €	5,87	160,00	14.080,00 €	25,34%	117,39 €	9,99%	13.962,61 €
Senior Consultant	37.500,00 €	50.625,00 €	25,01 €	9,07	190,00	4.560,00 €	8,21%	226,78 €	19,29%	4.333,22 €
MANAGER	45.000,00 €	60.750,00 €	30,01 €	12,67	240,00	12.000,00 €	21,60%	380,19 €	32,34%	11.619,81 €
PARTNER	70.000,00 €	94.500,00 €	46,69 €	2,27	450,00	2.700,00 €	4,86%	105,83 €	9,00%	2.594,17 €
Totale				**50,00**		**55.560,00 €**		**1.175,51 €**		**54.384,49 €**

ALLEGATO 10

PROGETTO GRANDE CON RPA 0,93

TASK	Descrizione lavoro	Partner	Manager	Senior Consultant	Consultant	Analyst 2	Analyst 1	Total hours	Gross Fees	Ore Consultant per attività
Rate (ora)		450,00 €	240,00 €	190,00 €	160,00 €	85,00 €	70,00 €	134	18.781,33 €	117
		6,40	**28,67**	**9,73**	**7,20**	**18,67**	**63,33**			
Understanding IT Environment		5	8	8	0	0,67	1,33	23	5840	36,50
Partner	Rilevazione ed aggiornamento ambiente IT che caratterizza il gruppo Z.	5,00						5,00	2.250	
Manager			8,00					8,00	1.920	
Senior Consultant				8,00				8,00	1.520	
Analyst 2						0,67		0,67	57	
Analyst 1							1,33	1,33	93	
GITC		0,27	2,67	1,73	7,20	10,13	25,33	47,33	4.876	30,48
Partner	Svolgimento dei controlli generali IT sugli applicativi CORE di Z (23 Applicativi + DB + OS + AD)	0,27						0,27	120	
Manager			2,67					2,67	640	
Senior Consultant				1,73				1,73	329	
Consultant					7,20			7,20	1.152	
Analyst 2						10,13		10,13	861	
Analyst 1							25,33	25,33	1.773	
ITAC		0,13	1,00	0,00	0,00	3,33	12,00	16,47	1.423	8,90
Partner	Controlli automatici	0,13						0,13	60	
Manager			1,00					1,00	240	
Analyst 2						3,33		3,33	283	
Analyst 1							12,00	12,00	840	
INTERFACCE		0,00	5,00	0,00	0,00	1,33	3,33	9,67	1.547	9,67
Manager	Analisi interfacce		5,00					5,00	1.200	
Analyst 2						1,33		1,33	113	
Analyst 1							3,33	3,33	233	
IPE		0,00	4,00	0,00	0,00	1,60	5,20	10,80	1.460	9,13
Manager	IPE		4,00					4,00	960	
Analyst 2						1,60		1,60	136	
Analyst 1							5,20	5,20	364	
Journal Entries Test		0,00	4,00	0,00	0,00	0,00	12,00	16,00	1.800	11,25
Manager	12 JET		4,00					4,00	960	

Analyst 1							12,00	12,00	840	
DATAWAREHOUSE		1,00	4,00	0,00	0,00	1,60	4,13	10,73	1.835	11,47
Partner	Analisi Datawharehouse	1,00						1,00	450	
Manager			4,00					4,00	960	
Analyst 2						1,60		1,60	136	
Analyst 1							4,13	4,13	289	

Ruolo	RAL	RAL+TASSE	Costo orario risorsa	Ore lavorate	Rate orario	Ricavo totale	Peso	Costo Totale	Peso	Margine totale
ANALYST	25.000,00 €	33.750,00 €	16,67 €	63,333333	70,00	66.500,00 €	47,97%	1.056,08 €	35,78%	65.443,92 €
ANALYST 2	28.000,00 €	37.800,00 €	18,68 €	18,666667	85,00	23.800,00 €	17,17%	348,62 €	11,81%	23.451,38 €
Consultant	30.000,00 €	40.500,00 €	20,01 €	7,2	160,00	17.280,00 €	12,46%	144,07 €	4,88%	17.135,93 €
Senior Consultant	37.500,00 €	50.625,00 €	25,01 €	9,7333333	190,00	6.460,00 €	4,66%	243,45 €	8,25%	6.216,55 €
MANAGER	45.000,00 €	60.750,00 €	30,01 €	28,666667	240,00	19.200,00 €	13,85%	860,42 €	29,15%	18.339,58 €
PARTNER	70.000,00 €	94.500,00 €	46,69 €	6,4	450,00	5.400,00 €	3,89%	298,81 €	10,12%	5.101,19 €
Totale				**134**		**138.640,00 €**		**2.951,46 €**		**135.688,54 €**

ALLEGATO 11

Calcolo costi e tempi di sviluppo per automazione 93%

Scaling Factors	very Low	Low	Nominal	High	Very High	Extra High
Precedentedness	6,2	4,96	3,72	2,48	1,24	
Development Flexibility	5,07	4,05	3,04	2,03	1,01	
Architecture/ Risk Resolution	7,07	5,65	4,24	2,83	1,41	
Team Cohesion	5,48	4,38	3,29	2,19	1,1	
Process Maturity	7,8	6,24	4,68	3,12	1,56	

$B = 1{,}01 + 0{,}01 * \sum SF$ =1,11 essendo esso maggiore di 1 esplica la presenza di diseconomie di scala.

COST DRIVER	*VERY LOW*	*LOW*	*NOMINAL*	*HIGH*	*VERY HIGH*	*EXTRA HIGH*
Prod.Attr						
RELY	0,82	0,92	1,00	1,10	1,26	
DATA		0,90	1,00	1,14	1,28	
CPLX	0,73	0,87	1,00	1,17	1,34	
RUSE		0,95	1,00	1,07	1,15	
DOCU	0,81	0,91	1,00	1,11	1,23	
Comp.Attr						
TIME			1,00	1,11	1,29	1,63
STOR			1,00	1,05	1,17	1,46
PVOL		0,87	1,00	1,15	1,30	
Pers.Attr.						
ACAP	1,42	1,22	1,00	0,85	0,71	
PCAP	1,34	1,16	1,00	0,88	0,76	
PCON	1,29	1,10	1,00	0,9	0,81	
APEX	1,22	1,10	1,00	0,88	0,81	
PLEX	1,19	1,12	1,00	0,91	0,85	
LTEX	1,20	1,10	1,00	0,91	0,84	
Project Attr.						
TOOL	1,17	1,09	1,00	0,90	0,78	
SITE	1,22	1,09	1,00	0,93	0,86	0,8
SCED	1,43	1,14	1,00	1,00	1,00	

EAF= PROD(CD)= 0,43

ALLEGATO 12

Costo trasferte

					Undertanding e Kickoff	
				Num_giorni	1	
Clienti piccoli	Numero clienti	Percentuale	Costo Trasferta	Num_risorse	3	Totale
Milano	82	34%			225,00 €	22.275,00 €
Lombardia	99	41%	50x+25x		978,00 €	40.098,00 €
Nord	41	17%	56x+150x+120x		1.068,00 €	11.748,00 €
Centro	11	5%	56x+180x+120x		1.188,00 €	13.068,00 €
Sud	11	5%	56x+220x+120x			
Totale	244	100%				87.189,00 €

					Undertanding e Kickoff	Test controlli		
				Num_giorni	1	15		
Clienti medi	Numero	Percentuale	Costo Trasferta	Num_risorse	3	2	Totale understanding e kickoff	Test controlli
Milano	42	49%						
Lombardia	25	29%	50x+25x		225,00 €	2.250,00 €	5.625,00 €	56.250,00 €
Nord	7	8%	56x+150x+120x		978,00 €	9.780,00 €	6.846,00 €	68.460,00 €
Centro	2	2%	56x+180x+120x		1.068,00 €	10.680,00 €	2.136,00 €	21.360,00 €
Sud	10	12%	56x+220x+120x		1.188,00 €	11.880,00 €	11.880,00 €	118.800,00 €
Totale	86	100%					26.487,00 €	264.870,00 €

					Undertanding e Kickoff	Test controlli		
				Num_giorni	1	30		
Clienti grandi	Numero	Percentuale	Costo Trasferta	Num_risorse	3	3	Totale understanding e kickoff	Tot Test controlli
Milano	16	80%						
Lombardia	2	10%	50x+25x		225,00 €	6.750,00 €	450,00 €	13.500,00 €
Nord	0	0%	56x+150x+120x		978,00 €	29.340,00 €	- €	- €
Centro	1	5%	56x+180x+120x		1.068,00 €	32.040,00 €	1.068,00 €	32.040,00 €
Sud	1	5%	56x+220x+120x		1.188,00 €	35.640,00 €	1.188,00 €	35.640,00 €
Totale	20	100%					2.706,00 €	81.180,00 €

	Senza Rpa	Con RPA 0,5	Con RPA 0,93
Piccoli	87.189,00 €	87.189,00 €	87.189,00 €
Medi	291.357,00 €	291.357,00 €	26.487,00 €
Grandi	83.886,00 €	83.886,00 €	2.706,00 €
TOTALE	462.432,00 €	462.432,00 €	116.382,00 €

ALLEGATO 13

Calcolo VAN e PB

RPA 0,5			
t	CF(t) Attualizzati	Investimento	VAN(t)
0	353.576,34 €	- 1.919.110,00 €	
1	321.433,03 €		
2	292.211,85 €		
3	265.647,14 €		
4	241.497,40 €		
5	219.543,09 €		- 578.777,50 €
6	199.584,62 €		
7	181.440,57 €		
8	164.945,97 €		
9	149.950,88 €		
10	136.318,98 €		253.463,53 €

RPA 0,93			
t	CF(t) Attualizzati	Investimento	VAN(t)
0	848.265,34 €	- 3.363.184,00 €	
1	771.150,31 €		
2	701.045,73 €		
3	637.314,30 €		
4	579.376,64 €		
5	526.706,04 €		- 147.590,98 €
6	478.823,67 €		
7	435.294,24 €		
8	395.722,04 €		
9	359.747,31 €		
10	327.043,01 €		1.849.039,29 €